DOCUMENT RESUME

ED 441 401 IR 020 433

| | |
|---|---|
| TITLE | Commission on Child Online Protection (COPA) Report to Congress [and] Personal Statements of COPA Commissioners. |
| PUB DATE | 2000-10-20 |
| NOTE | 94p.; For appendices to report, see IR 020 434. For full text of personal statements: http://www.copacommission.org. |
| PUB TYPE | Reports - Evaluative (142) |
| EDRS PRICE | MF01/PC04 Plus Postage. |
| DESCRIPTORS | Access to Information; *Child Safety; *Children; Federal Legislation; Federal Regulation; Freedom of Speech; *Information Policy; Information Technology; *Internet; Policy Formation; Pornography; Privacy |
| IDENTIFIERS | Acceptable Use Policy; Commission on Online Child Protection; Filters; First Amendment |

ABSTRACT

In October, 1998, Congress enacted the Child Online Protection Act and established the Commission on Online Child Protection (COPA) to study methods to help reduce access by minors to certain sexually explicit material, defined in the statute as harmful to minors. Congress directed the Commission to evaluate the accessibility, cost, and effectiveness of protective technologies and methods, as well as their possible effects on privacy, First Amendment values, and law enforcement. This report responds to the Congressional request. The Commission studied a wide range of child-protective technologies and methods, including filtering and blocking services; labeling and rating systems; age verification efforts; the possibility of a new top level domain for harmful-to-minors material; "greenspaces" containing only child-appropriate materials; Internet monitoring and time-limiting technology; acceptable use policies and family contracts; online resources providing access to protective technologies and methods; and options for increased prosecution against illegal online material. The report includes the following sections: (1) Introduction; (2) Technologies and Methods; (3) Recommendations; (4) Affirmative Defenses; (5) Proposed Future Work; and (6) Conclusion. A companion volume, "Personal Statements of COPA Commissioners," is appended. (MES)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 441 401

# Commission on Child Online Protection (COPA)

## REPORT TO CONGRESS

**October 20, 2000**

BEST COPY AVAILABLE

IR020433

K. Litterot

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

- This document has been reproduced as received from the person or organization originating it.
- Minor changes have been made to improve reproduction quality.
- Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

## COMMISSION ON ONLINE CHILD PROTECTION

Donald Telage, Network Solutions Inc. –
*Chairman*
Stephen Balkam, Internet Content Rating Association
John Bastian, Security Software Systems
Jerry Berman, Center for Democracy & Technology
Arthur H. DeRosier, Jr., Rocky Mountain College
J. Robert Flores, National Law Center for Children and Families
Albert F. Ganier III, Education Networks of America
Michael E. Horowitz, Department of Justice
Donna Rice Hughes, Author, Kids Online/Founder, Protectkids.com
William M. Parker, Crosswalk.com
C. Lee Peeler, Federal Trade Commission
Gregory L. Rohde, Department of Commerce/NTIA
C. James Schmidt, San Jose State University
William L. Schrader, PSINet Inc.
Larry Shapiro, Walt Disney Internet Group
Srinija Srinivasan, Yahoo! Inc.
Karen Talbert, Nortel Networks
George Vradenburg III, America Online, Inc.

## ACKNOWLEDGEMENTS

This Commission was not funded. Its operations were made possible by contributions of time by numerous individuals and companies, and by monetary grants from Network Solutions. Inc.; Yahoo! Inc.; America Online, Inc.; Education Networks of America; and PSINet. These contributions of time and funds were supplied unconditionally and with no expectation or receipt of consideration in any form from the Commission, under statutory gifts and grants authority. The Commission further thanks America Online, Inc.; Yahoo ! Inc.; San Jose State University, San Jose, California; the University of Richmond, Richmond, Virginia; McGuire Woods Consulting; and US Postal Service, for donating hearing facilities or related assistance; Congressional Internet Caucus Advisory Committee for donating web site design and hosting; and Alice Ganier for preparing the appendices.

Gifts and grants were used in part to pay Dittus Communications for essential organizational services. The Commission thanks Dittus, particularly Kristin Litterst, Jennifer Moire, Caroline Dietz, Marcy Stansbury, Kyle Pirnat, Jack Choate, Rob Gieser, Kathleen Mikitko, and Peggy O'Neill for services above and beyond what we could reasonably have expected.

Finally, we thank David R. Johnson and Susan P. Crawford of the law firm of Wilmer, Cutler & Pickering, who served as legal staff to Chairman Donald Telage. Their organizational and strategic advice was essential to the Commission's success.

## LETTER OF TRANSMITTAL

**October 20, 2000**

To The Congress of the United States:

On behalf of the Commission on Online Child Protection, I am pleased to transmit to Congress the Commission's final Report reflecting its study of technologies and methods designed to reduce access by minors to harmful to minors material on the Internet. This Report fulfills the Commission's statutory mandate to report the results of its study no later than October 21, 2000.

I would like to take this opportunity to recognize the outstanding efforts of eighteen Commissioners who devoted their time and energies to thoughtful consideration of the questions presented to the Commission by Congress. I am proud to have served in the company of such a distinguished group, and I commend the dedication and collegiality of the Commissioners.

Sincerely,

D. N. Telage

Donald N. Telage
Executive Advisor for Global Internet Strategy,
Network Solutions Inc.
Chairman,
Commission on Online Child Protection

## TABLE OF CONTENTS


Executive Summary .....7

I. Introduction.....11

II. Technologies and Methods.....14
- A. Common Resources and Parental Education.....17
- B. Filtering/Blocking.....19
- C. Labeling and Rating Systems.....23
- D. Age Verification Systems.....25
- E. New Top-Level Domain/Zoning.....28
- F. Other Technologies or Methods.....32

III. Recommendations.....39

IV. Affirmative Defenses.....46

V. Proposed Future Work.....47

VI. Conclusion.....48


Appendix

See companion volume containing personal statements of individual Commissioners. The personal statements are also available on the Web site at www.copacommission.org.

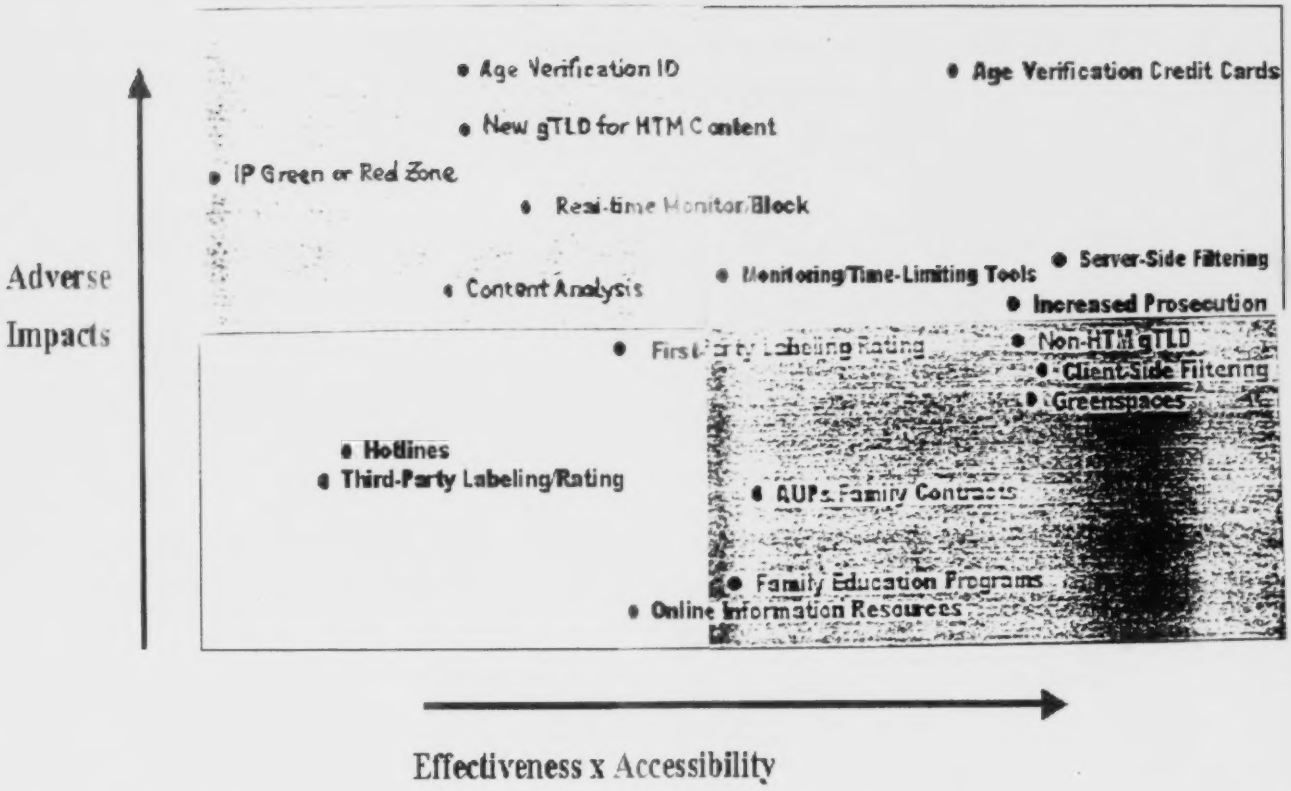
## EXECUTIVE SUMMARY

The experience of America's children online has been at the forefront of concern for families and policymakers since the Internet first became widely available. The Internet is revolutionizing access to information, providing undeniable benefit to consumers and commerce. Nonetheless, it risks exposing children to sexually explicit material that many believe is inappropriate or harmful.

In October 1998 Congress enacted the Child Online Protection Act and established the Commission on Online Child Protection to study methods to help reduce access by minors to certain sexually explicit material, defined in the statute as harmful to minors. Congress directed the Commission to evaluate the accessibility, cost, and effectiveness of protective technologies and methods, as well as their possible effects on privacy, First Amendment values and law enforcement. This report responds to the Congressional request.

The Commission studied a wide range of child-protective technologies and methods, including filtering and blocking services; labeling and rating systems; age verification efforts; the possibility of a new top-level domain for harmful to minors material; "greenspaces" containing only child-appropriate materials; Internet monitoring and time-limiting technologies; acceptable use policies and family contracts; online resources providing access to protective technologies and methods; and options for increased prosecution against illegal online material.

The following "scattergram" provides a snapshot of the Commission's analysis of the positive and negative attributes of each of the technologies and methods evaluated in this report. The horizontal axis shows scores for the combination of effectiveness and accessibility. The vertical axis shows cumulative scores for user cost, cost to sources of otherwise lawful harmful to minors materials and adverse impacts on privacy, First Amendment values and law enforcement.




BEST COPY AVAILABLE

Technologies and methods identified in the lower right quadrant are most effective and accessible while imposing fewer costs and adverse impacts. Those identified in the upper left quadrant are relatively ineffective and create the most adverse effects.

After consideration of the information gathered through hearings and comments filed by a wide range of parties, the Commission concludes that no single technology or method will effectively protect children from harmful material online. Rather, the Commission determined that a combination of public education, consumer empowerment technologies and methods, increased enforcement of existing laws, and industry action are needed to address this concern. The Commission's specific recommendations are as follows:[1]

***Public Education:***

- Government and the private sector should undertake a major education campaign to promote public awareness of technologies and methods available to protect children online.

- Government and industry should effectively promote acceptable use policies.

***Consumer Empowerment Efforts:***

- Resources should be allocated for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies.

- Industry should take steps to improve child protection mechanisms, and make them more accessible online.

- A broad, national, private sector conversation should be encouraged on the development of next-generation systems for labeling, rating, and identifying content reflecting the convergence of old and new media.

- Government should encourage the use of technology in efforts to make children's experience of the Internet safe and useful.

***Law Enforcement:***

- Government at all levels should fund, with significant new money, aggressive programs to investigate, prosecute, and report violations of federal and state obscenity laws, including efforts that emphasize the protection of children from accessing materials illegal under current state and federal obscenity law.

---

[1] This is an abbreviated version of the recommendations. The full text of the Commission's recommendations can be found at pp. 39 to 46 of the Report.

- State and federal law enforcement should make available a list, without images, of Usenet newsgroups, IP addresses, World Wide Web sites or other Internet sources that have been found to contain child pornography or where convictions have been obtained involving obscene material.

- Federal agencies, pursuant to further Congressional rulemaking authority as needed, should consider greater enforcement and possibly rulemaking to discourage deceptive or unfair practices that entice children to view obscene materials, including the practices of "mousetrapping" and deceptive meta-tagging.

- Government should provide new money to address international aspects of Internet crime, including both obscenity and child pornography.

***Industry Action:***

- The ISP industry should voluntarily undertake "best practices" to protect minors.

- The online commercial adult industry should voluntarily take steps to restrict minors' ready access to adult content.

**Conclusion**

The child-protective technologies and methods evaluated by the Commission provide an important but incomplete measure of protection from harmful to minors material online. The efforts recommended in this report, if implemented by industry, consumers, and government, will result in significant improvements in protection of children online.

# I. INTRODUCTION

The protection of America's children online has been a powerful motivating issue for policymakers since the Internet became widely available in our nation's homes, schools, and libraries. The Internet promises to revolutionize access to information, create new forms of social interaction, promote economic opportunity, and reinvigorate civic discourse. Yet this same technology risks exposing children to material, particularly material of a sexually-explicit nature, that many believe is inappropriate or harmful to their development.

Policymakers have found no easy and effective response to the problem of protecting children online. Laws directly restricting potentially harmful content online have encountered technical and Constitutional difficulties. The effectiveness of domestic laws in the global context of the Internet has been called into question, and U.S. courts have struck down these same laws for infringing the First Amendment rights of American adults. These difficulties have led to a cycle of legislation, litigation, and court action that has provided little in the way of solutions for families seeking to deal with inappropriate content on the Internet.

The mission of the Commission on Online Child Protection is to evaluate potential solutions to the problem of restricting children's access to inappropriate material on the Internet. In doing so, the Commission's goal has been to assess these solutions in light of the technical realities of the Internet and legal concerns raised by First Amendment, privacy and law enforcement interests.

## A. The Commission's Mandate

In October 1998 Congress enacted the Child Online Protection Act (COPA) and established the Commission on Online Child Protection[2] to study "methods to help reduce access by minors to material that is harmful to minors on the Internet."[3] Congress directed the Commission to evaluate the accessibility, cost,

---

[2] The Commission is a temporary, 19-member organization composed of representatives of industry and government. 47 U.S.C. § 231 note.

[3] The term harmful to minors is defined as any "communication. . . that is obscene or that –

(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

and effectiveness of protective technologies and methods, as well as their possible effects on privacy and law enforcement. It asked the Commission to file a report to Congress by October 21, 2000 containing its evaluation of these technologies and methods, making recommendations for further legislative or administrative action, and identifying which technologies or methods might meet the requirements for use as affirmative defenses to civil and criminal provisions of the COPA.

This report responds to the Congressional request. Because the Commission membership was not finally established until the end of 1999, the Commission's first meeting was held March 7, 2000. Thereafter, the Commission gathered input for its deliberations through three hearings held this summer in Washington, DC; Richmond, VA; and San Jose, CA; and through written submissions by the public. It also established a web site to provide the public with information on the Commission's activities and mission and to accept public comment.

## B. The Legal Context

In considering technologies and methods for protecting children on the Internet, the Commission has been particularly concerned with their impact on speech. Congress, along with several states, has passed laws attempting to limit children's access to "indecent" or harmful to minors content online.[4] In 1997, the Supreme Court held unconstitutional the indecency provisions of the first of these, the Communications Decency Act of 1996. Enforcement of the criminal provisions of the second of these, COPA, was enjoined by federal district and appellate courts on constitutional grounds and remains the subject of litigation. Based on the records before them, the courts in these cases cited the impact of content restrictions on the First Amendment rights of adults. Courts have applied strict scrutiny to these Internet statutes and found that the statutes did not utilize

---

(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) taken as a whole, lacks serious literary, artistic political, or scientific value for minors." 47 U.S.C. 231(e)(6).

For the purpose of this statute, a minor is a person under 17. *Id.* at 231(e)(7).

[4] E.g., VA. CODE ANN. § 18.2-391 (Internet content "harmful to juveniles"); N.M. STAT. ANN. § 30-37-3.2 (dissemination of material that is harmful to a minor by computer).

the "least restrictive means" most narrowly tailored to protect children effectively without unacceptably restricting free speech.

Even when not mandated, protective technologies and methods may have the effect of restricting speech. Protective technologies may be implemented at a variety of points -- not only on home computers, but in such places as public libraries and businesses, and by Internet service providers. Used in these ways, even voluntarily implemented protective methods reduce access to fully protected speech. Accordingly, a key question for the Commission has been: What are the most effective means of serving the public's interest in protecting children online that have the least potential adverse impacts on protected adult speech?

### C. The Internet Context

The Commission has also been mindful of the unique characteristics of the Internet and its impact on the ability to protect children. The Internet's technical architecture creates new challenges as well as opportunities for children and families. Material published on the Internet may originate anywhere, presenting challenges to the application of the law of any single jurisdiction. Methods for protecting children in the U.S. must take into account this global nature of the Internet. In addition, thousands of access providers and millions of potential publishers provide content online. Methods to protect children from content harmful to minors must be effective in this diverse and decentralized environment, including the full range of Internet activity such as the Web, email, chat, instant messaging, and newsgroups.

The Internet is also rapidly changing and converging with other, more traditional media. Effective protections for children must accommodate the Internet's convergence with other media and extend to new technologies and services offered on the Internet, such as instant messaging, interactive television, or broadband access. And unlike one-way broadcast media, the Internet is inherently multi-directional and interactive. This interactivity may create new possibilities for Internet users to exercise greater control over the content they see online and for content producers to target their audience. While these characteristics of the Internet challenge traditional policy-making, these very features also are the source of the Internet's promise and success.

The Commission also is aware that many families feel unfamiliar with the Internet, and find it harder to protect their children online than they do in the real world. Differences in language or culture and resource limitations may challenge families' ability to protect their children online. Further, children may access the Internet in places other than their own home – at school, at libraries and at the home of friends, relatives and caregivers, where the direct supervision of parents may not be possible.

### D. The Commission's Assessment and Report

This report considers the following protective technologies and methods: filtering and blocking services; labeling and rating systems; age verification efforts; the possibility of a new top-level domain for harmful to minors material; "green" spaces containing only child-appropriate materials; Internet monitoring and time-limiting technologies; acceptable use policies and family contracts; online resources providing access to protective technologies and methods; and options for increased prosecution against illegal online material.

This report reflects the Commission's analysis and conclusions. Following this introduction are 18 sections, each containing the Commission's analysis of a specific technology or method, including a description of the technology or method;[5] a bar chart setting forth a summary of the COPA Commission's rating of the technology or method's effectiveness, accessibility and costs; and a brief discussion of the technology or method's advantages and disadvantages. The recommendations that follow represent the Commission's analysis of child-protective technologies as a whole, as well as suggestions for Congress and industry.

This Commission acted under significant time restraints with limited resources. With more time and appropriated funding, it would have conducted independent evaluations of new technologies, and held further hearings that would likely have elicited more useful information. Nonetheless, the record provides ample support for the evaluations and recommendations that follow.

---

[5] The report evaluates categories of technologies and methods, not specific products. It may offer examples of specific technologies, but it is not designed to suggest a preference for any current product.

## II. TECHNOLOGIES AND METHODS

The Commission[6] rated each technology or method in light of both its current effectiveness and near-term potential effectiveness, relative to other technologies and methods, in reducing access by children to harmful to minors materials (when used along with other related technologies and methods). Except where explicitly noted, the Commission's inquiry focused primarily on use of a technology or method in the home and other private environments. Although COPA by its terms applies strictly to the Web, the Commission examined use of a technology or method in other Internet-related contexts, such as email, chat, instant messaging, and newsgroups.

Ratings were made on a scale of zero to ten regarding the relative effectiveness, accessibility, user cost, cost imposed on sources of lawful harmful to minors materials, and adverse impacts on privacy, First Amendment values, and law enforcement. The Commission assumed, for each technology and method rated, a high quality example of that technology and method was being assessed (and not any particular product). The Commission notes that further analysis could make substantial differentiation between sub-categories within any particular technology and method -- to allow study of important differences in particular types of implementations or in different environments.

The "effectiveness" rating, in general, assumes the technology is currently available. "Accessibility" again assumes the technology is currently available, and is designed to measure whether the technology or method is easy to find, implement, and use. "User cost" refers to costs to consumers and other users, and, in some cases, costs spread across all users by means of taxes. "Source cost" refers to costs imposed on the sources of otherwise lawful adult content that would be deemed harmful to minors under COPA. "Privacy" refers to potential and actual risks to information that may or may not be kept secure. "First Amendment" refers to impact on overall First Amendment values concerning the free flow of information, rather than narrowly to actions taken by

---

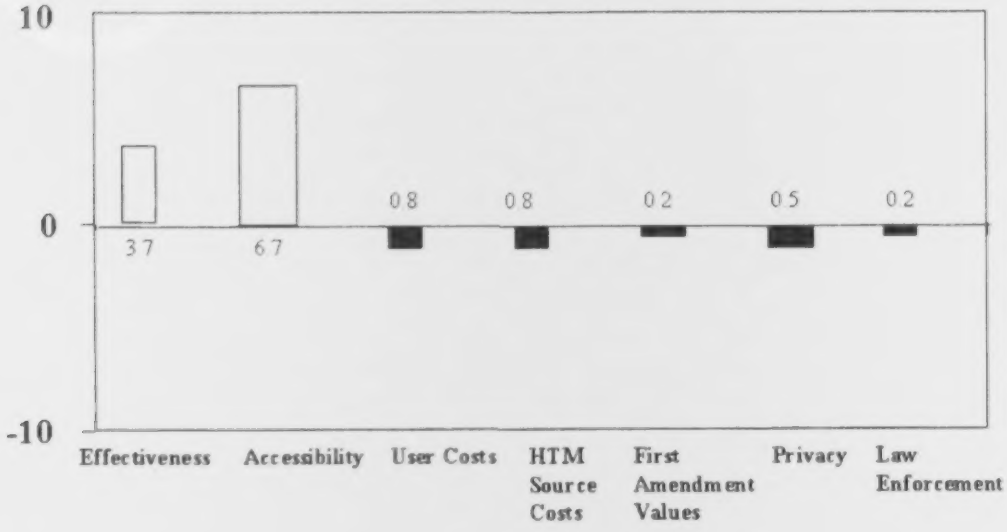
[6] The government representatives to the Commission were appointed in an "ex officio" capacity. This is an advisory role. Accordingly, they did not rate the technologies and methods, vote on the recommendations, or approve this report.

governmental actors. The Commission directly rated only adverse effects on law enforcement but comments will note where a technology or method could create specific positive benefits for law enforcement.

## A. Common Resources and Parental Education

### 1. Online information resources

Collection of information regarding technologies and methods that can protect children and publication of such information on an open web page, with links to additional pertinent materials.[7]




### Commentary

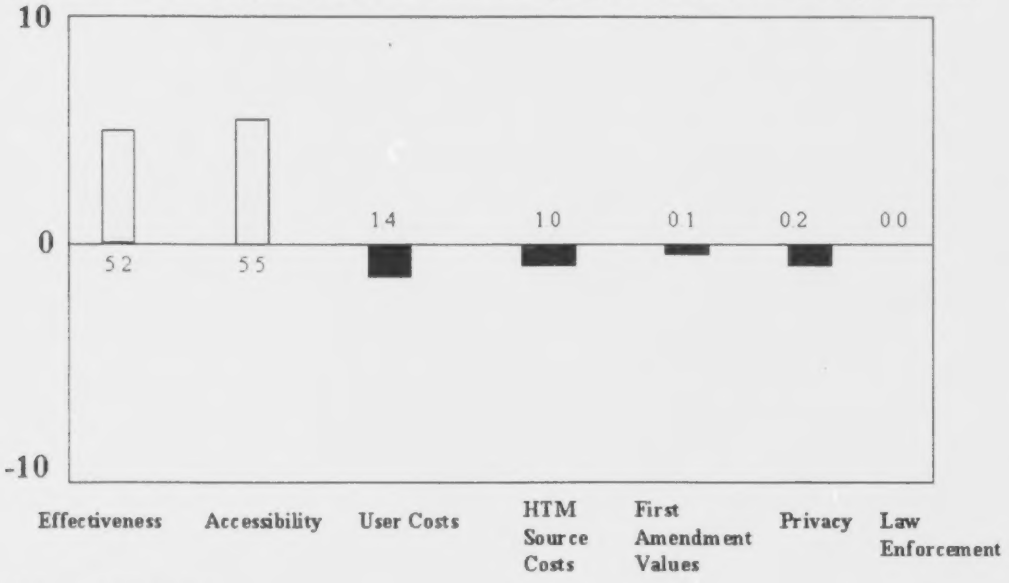
- Internet companies have made substantial efforts to make these online information resources available. While not directly preventing access to harmful to minors materials, online information resources are essential to protecting children, as they can effectively provide access to technologies, information for families online, and hotlines to reach and report to authorities. Easily accessible online, the "one-click-away" approach is well-designed to make sure that notice of available technologies is provided at common points of entry to the Internet.
- These provide substantial benefits with little adverse impact on privacy, free speech, or costs imposed on users and publishers of otherwise lawful harmful to minors materials. These can have a potential positive effect on law enforcement by fostering greater information flow.

---

[7] The following bar chart sets forth a summary of the COPA Commission's rating of this technology or method's effectiveness, accessibility, and costs. See p. 15 for a description of the rating system.

## 2. Family Education Programs

Active outreach to educate families about both opportunities and dangers of the Internet, as well as the technologies and practices that can optimize a child's experience online -- with a goal of encouraging families' involvement with their children's online experience and wider adoption of common sense practices.



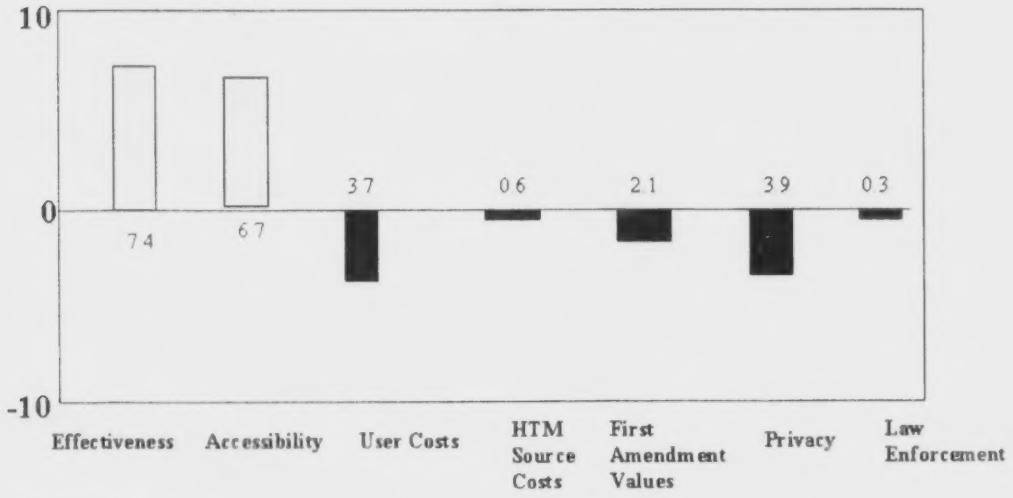

### Commentary

- Good educational programs are readily accessible online.
- As with online resources, family education programs do not themselves directly prevent minors' access to harmful to minors materials, but they are an essential part of an overall solution. As families are the first line of defense in raising and protecting children, education programs can be highly effective in giving caregivers needed information about online risks and protection methods, and access to technologies and ways to get help.
- Availability of offline education materials varies from community to community.
- Offline education programs may be especially effective at reaching families that are not currently online, and may serve as a catalyst to encourage parents and other caretakers to take a more active role in childrens' online experience.
- Non-English language versions of these programs are less readily available.
- Family education imposes little or no cost on publishers of otherwise lawful harmful to minors materials and creates little adverse impact on privacy, First Amendment values, or law enforcement.

## B. Filtering/Blocking

### 3. Server-side filtering using URL[8] lists

Voluntary use by Internet Service Providers and Online Services of server software that denies access to particular content sources (identified by uniform resource locators) that have been selected for blocking. The selection of the blocked list can rely upon automated processes, human review, and user options. The list of blocked URLs may or may not be disclosed. The list is regularly updated at the server.




### Commentary

- Server-side filtering using URL lists is available now from numerous sources.
- Relative to other technologies, the best of these technologies can be highly effective in directly blocking access to global harmful to minors content on the Web and also on newsgroups, email and chat rooms. Server-side filters may be more easily implemented on a wide scale than client-side filters and may be more difficult for children to defeat.
- Due to rapid growth in Internet content, server-side filters using URL lists may not be perfectly effective in blocking. Server side technologies are accessible and easy to install and require few actions by the family. Different systems offer different degrees of customizability to reflect parental values, though many offer less control than client-side systems.
- Moderately costly to end-users, while costs to publishers of otherwise lawful harmful to minors materials are low.

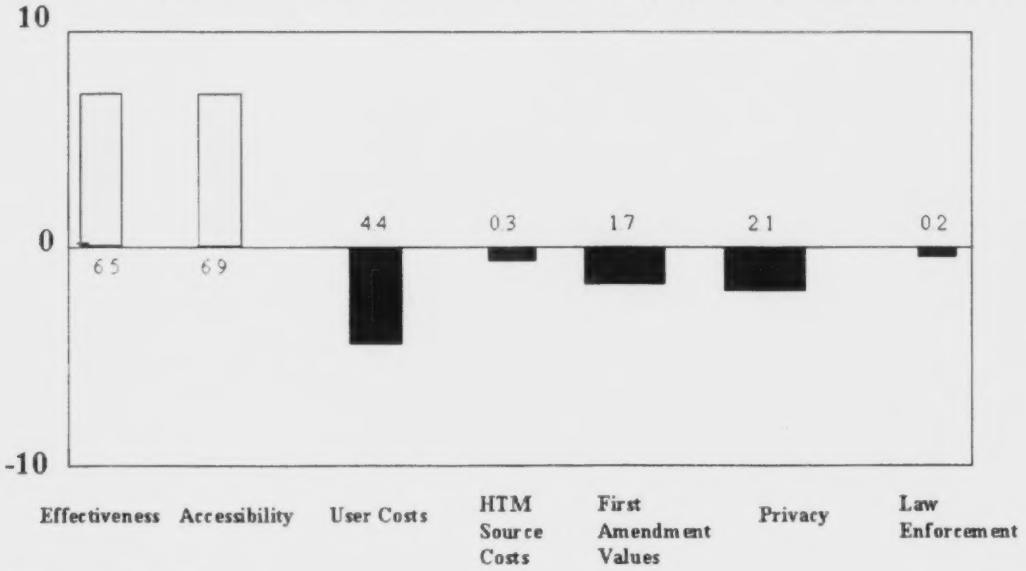
---

[8] URL" is the abbreviation for "universal resource locator" and refers to the address of an Internet site. For example, this Commission's URL is "www.copacommission.org."

- This technology raises First Amendment concerns because of its potential to be over-inclusive in blocking content. Concerns are increased because the extent of blocking is often unclear and not disclosed, and may not be based on parental choices. There is less of an impact on First Amendment concerns if filtering criteria are known by the consumer or other end-user and if filters are customizable and flexible.
- Central collection of preference and access information raises privacy concerns, as compared with client-side filtering systems.
- These systems could work with labeling regimes and greenspaces.
- There are significant concerns about First Amendment values when server-side filters are used in libraries and schools.

## 4. Client-side filtering using URL lists

Voluntary use by end users of software that causes the browser not to download content from specified content sources. The list of blocked sites may originate from both the software supplier and/or from decisions by the user. The list may be updated periodically by means of a download from the site of the software provider. The list may or may not be disclosed. A denial of access may be overridden with the use of a password controlled by a parent. The PC-based software may also filter out email or instant messaging from unapproved sources.

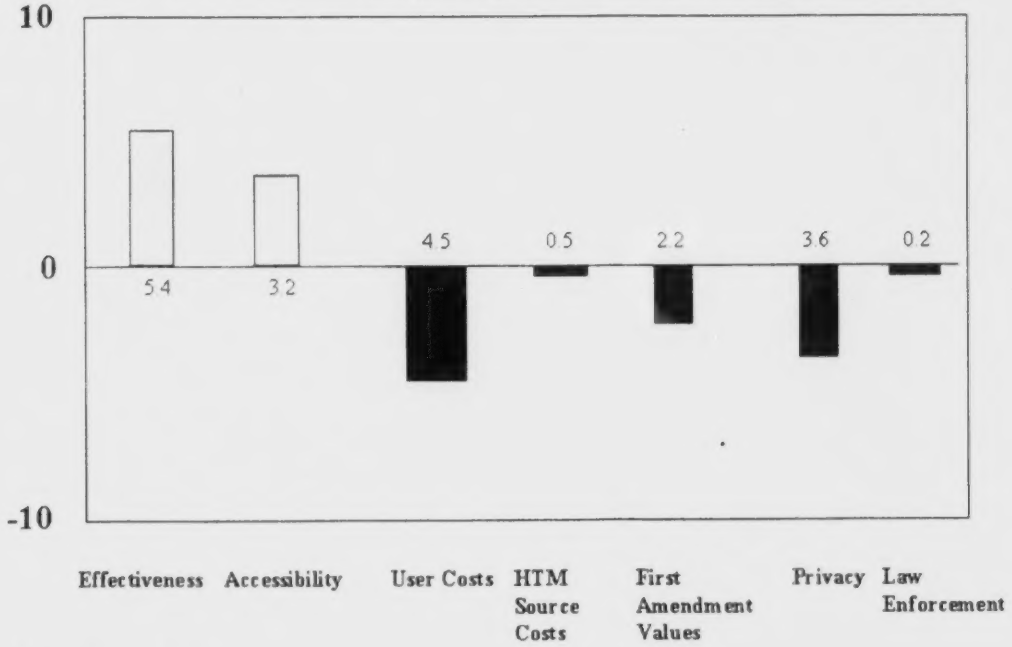



### Commentary

- These systems are widely available from retail and other outlets. They require some effort by the end user to configure and update.
- Client-side filtering can be effective in directly blocking access to global harmful to minors content on the Web, in newsgroups, in email and in chat rooms. While often more flexible than server-side filters, client-side filters may be easier for children to defeat. Additionally, they require updating to keep pace with the global proliferation of harmful to minors content.
- Due to rapid growth in Internet content, client-side filters using URL lists may not be fully effective in blocking.
- This technology raises First Amendment concerns because of its potential to be over-inclusive in blocking content. Concerns are increased because the extent of blocking is often unclear and not disclosed. Still, many of these can be customized based on family choice.
- This technology is moderately costly to end users, while costs to publishers of harmful to minors material are low.
- The privacy impact of client-side filtering is lower than that for server-side filtering, as data resides locally.
- These systems have little impact on law enforcement.

## 5. Filtering (server- and client-side) using text-based content analysis

Voluntary use of some combination of PC-based software and server software that conducts (when necessary) real time analysis of the content of a web site and filters out content sources that fit some algorithm. The Commission assessed only text-based systems, which seem more promising than image analysis. Such a system may be able to analyze email and attachments. The end user may or may not be informed of the nature of the algorithm and may or may not have full information regarding what is being excluded.



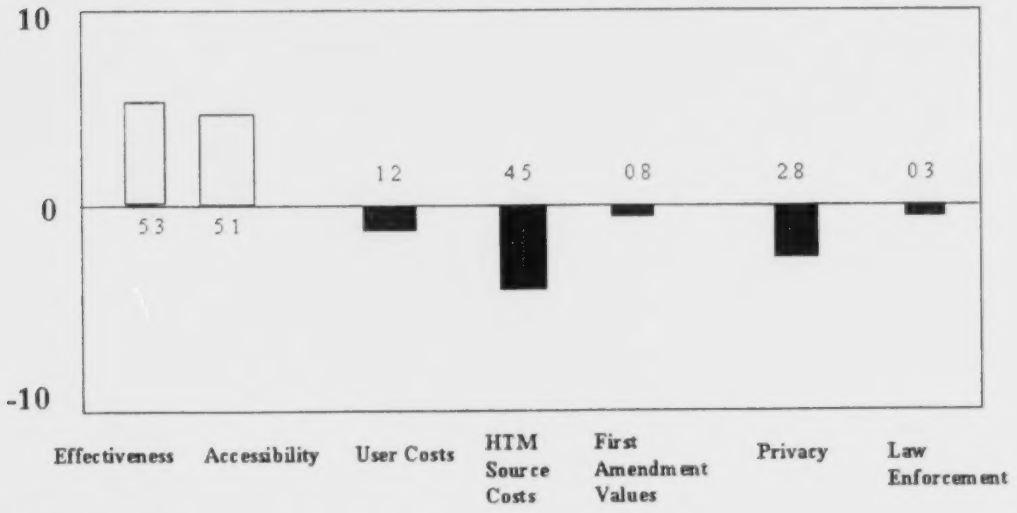

### Commentary

- This is an emergent technology that is not yet widely available.
- This technology may work well on text, but to be fully effective it must work on a combination of text and images. Application in real-time makes it easier for filtering to keep up with the growing and changing content on the Internet.
- This technology raises First Amendment concerns because of its potential to be over-inclusive in blocking content. Concerns are increased because the extent of blocking is often unclear and not disclosed. Client-side systems may be customized based on family choice.
- These technologies are moderately costly to consumers and other end-users. Adverse impacts to First Amendment values and costs to publishers stem from risk of over-inclusive blocking.
- Server-side products may raise privacy concerns based on the presence of centralized data about a user's preferences and access patterns.

## C. Labeling and Rating Systems

### 6. First-party labeling/rating

Voluntary action by content sources to indicate that a site or particular content meets a particular standard or fits a particular category. The "label" can take the form of a metatag, or entry into a database listing, or display of a seal. The use of a label may be audited. For purposes of considering this technology, the Commission will assume that the voluntary labeling scheme would identify material that is harmful to minors and thereby allow others to filter or block such material.

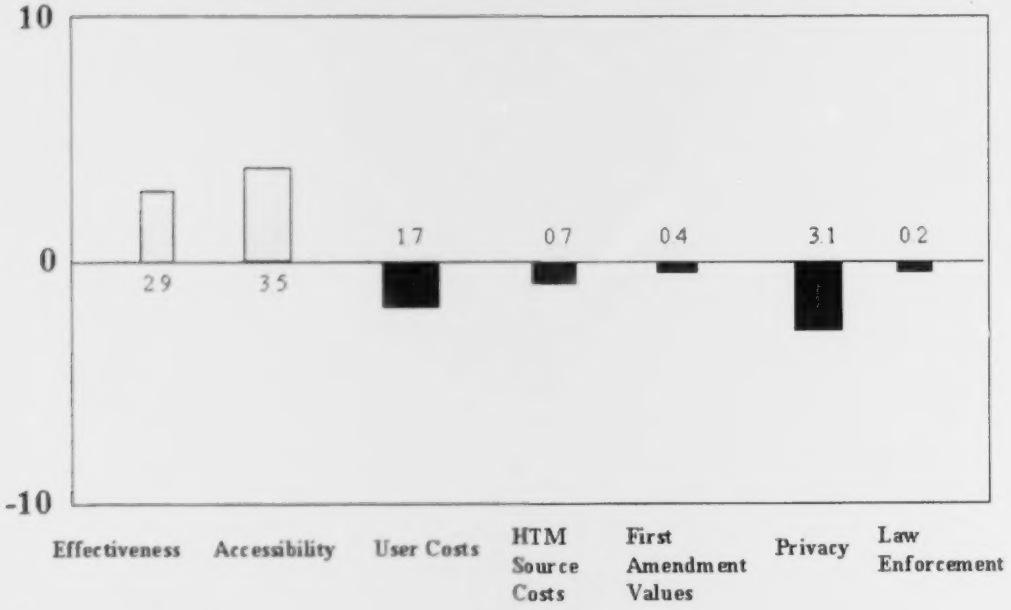



### Commentary

- Although potentially effective if widely used, this method has not been adopted by many Web publishers.
- The effectiveness of voluntary first-party labeling is limited because it is dependent in part on widespread adoption.
- This is a low cost method for consumers and other end-users; browsers that look for self-labels do so at no cost.
- This method may impose costs on all sources of harmful to minors material, depending on the complexity of the labeling or rating design and on requirement to label or rate each web page.
- This method raises First Amendment concerns due to the financial cost to constitutionally protected sites, blocking of unlabelled sites, and the threat that voluntary labeling regimes might be made mandatory.
- This method may facilitate creation of lists of child-appropriate sites and greenspaces.

## 7. Third-party labeling/rating

Voluntary action by third parties to review content sources and to associate labels or ratings with such sources so as to enable filtering or blocking by others. The review may involve some automated parsing and some human judgment. For purposes of considering this technology, the Commission will assume that the labeling and related filtering may involve various "categories" established by private parties and that no affirmative action is required by a content source.



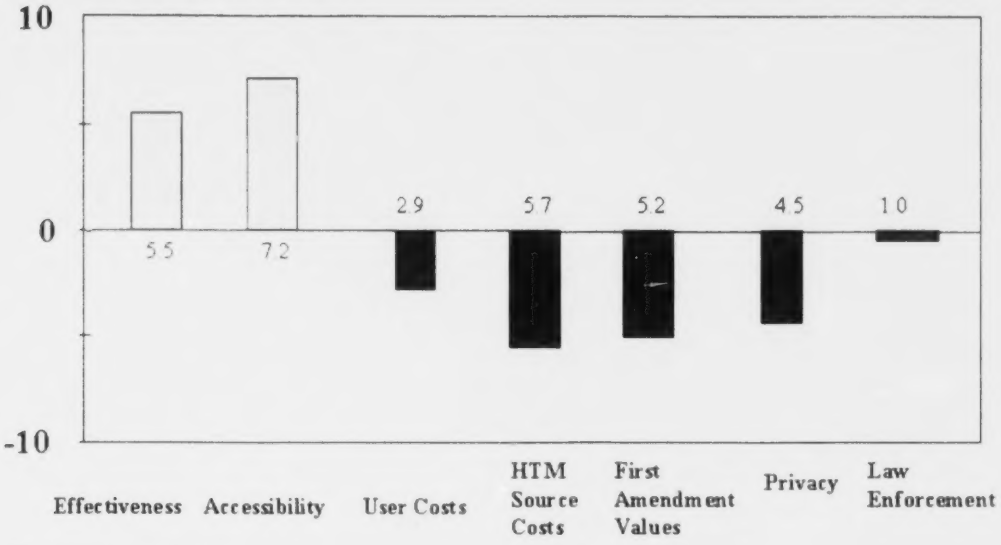

### Commentary

- This approach is similar to that followed in the motion picture industry, where a third party assigns a rating to each film. It is not widely used on the Internet at this time. It requires that third parties engage in rating a large number of sites.
- Third-party labeling/rating could be effective if third parties, such as advocacy groups, were to decide to engage in this process, or if the adult-content industry were to cooperate in establishing a third-party labeling regime. Any such scheme will be challenged by the immense scope of the content to be rated and constant changes in web site content.
- This technology has the potential for coordination with rating schemes in other media. At this time, however, there is no clear business model for this approach on the Internet.
- First Amendment concerns derive from the fact that labels assigned to content by third parties will reflect cultural or social standards that may not be shared by others.
- Third party labeling would have little or no adverse impact on privacy or on law enforcement.

## D. Age Verification Systems

## 8. Age Verification Systems based on credit cards

Use by a content source of a system to condition access to a web page (or pushed content) on the end user's ability to provide a credit card number. The number may or may not be verified as relating to a valid card (it may not be used for charging a fee) and may or may not be further analyzed to assure that the holder of the card is an adult.



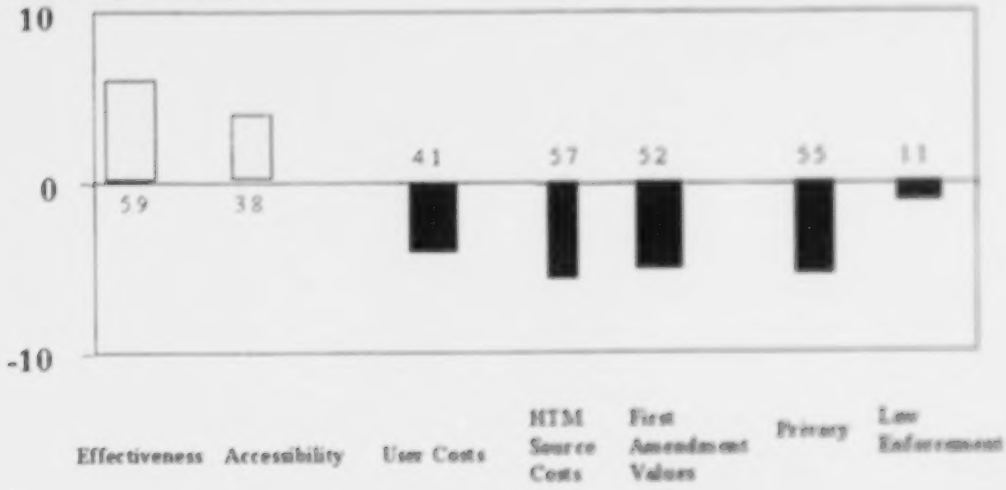

### Commentary

- Use of a credit card verification system to access harmful to minors material can be effective to protect minors from accessing some harmful to minors material. A large number of sites operated by the commercial online adult content industry use this system now, but they may still make some images available for free.
- This system's limitations include the fact that some children have access to credit cards, and it is unclear how this system would apply to sites outside the US. It is not effective at blocking access to chat, newsgroups, or instant messaging. Delay in billing means that unauthorized access to harmful to minors materials could occur.
- Credit card systems are readily available, but it may be difficult or burdensome for small or non-commercial sites to implement card verification systems. This system would make some content inaccessible to those users without credit cards.
- This approach imposes moderate costs on consumers and other end-users, who must have a credit card and accept risks in providing it to sites. This approach imposes high costs on publishers, who must pay to verify cards. Use for verification without putting through a charge is viewed with disfavor by the credit card industry.

- Collection of individually-identifiable information at central points via this system poses privacy risks.
- Adverse impacts on First Amendment values result from cost to publishers and chilling effect of identifying users before providing access.
- Central collection of credit card numbers coupled with the "embarrassment effect" of reporting fraud may have adverse effects on law enforcement.

## 9. Age Verification System based on independently-issued ID

Use by a content source of a system to condition access to a web page (or pushed content) on the end user's use of a password protected identifier that is issued (by a third party) only to those who have presented some credentials indicating adult age.



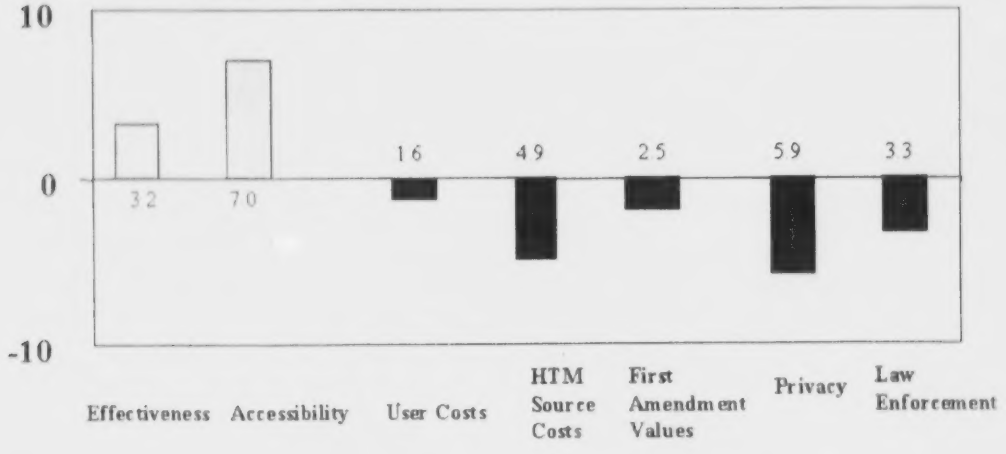

### Commentary

- A number of sources provide this service on a commercial basis at this time. For sites that utilize it, this approach is generally effective at preventing access by children. Overall effectiveness of this approach depends on the extent of control over access to the identification codes and the extent of adoption. This approach is not effective at blocking access to chat, newsgroups, or instant messaging.
- This approach imposes moderate costs on users, who must get an I.D. It imposes high costs on content sources that must install systems and might pay to verify I.D.s.
- The adverse effect on privacy could be high. It may be lower than for credit card verification if I.D.s are separated from personally-identifiable information.
- Uncertainty about the application of a harmful to minors standard increases the costs incurred by harmful to minors sites in connection with such systems.
- An adverse impact on First Amendment values arises from the costs imposed on content providers, and because requiring identification has a chilling effect on access. Central collection of credit card numbers coupled with the "embarrassment effect" of reporting fraud and the risk that a market for I.D.s would be created may have adverse effect on law enforcement.

## E. New Top-Level Domain/Zoning

### 10. Establishment of a gTLD for harmful to minors content

Creation for voluntary use of a new top level domain (e.g., .xxx or .adult) the use of which would be understood to signify that materials on web pages located in such domain (and email coming from such domain) are harmful to minors materials -- and the existence of which would make it easy for browsers or ISPs to filter out all material so located.




### Commentary

- This method is technically feasible but such a domain does not currently exist. It requires that ICANN[9] establish such a new top-level domain.
- This system may be only moderately effective because of questions about whether harmful to minors content sources would locate material exclusively in the .xxx domain. This method also may be inapplicable to chat, email, newsgroups and instant messaging. Use of the domain name system to implement policy raises concerns.
- Privacy and First Amendment concerns may be raised by the clear identification of a "red light district" and the stigma involved in being found

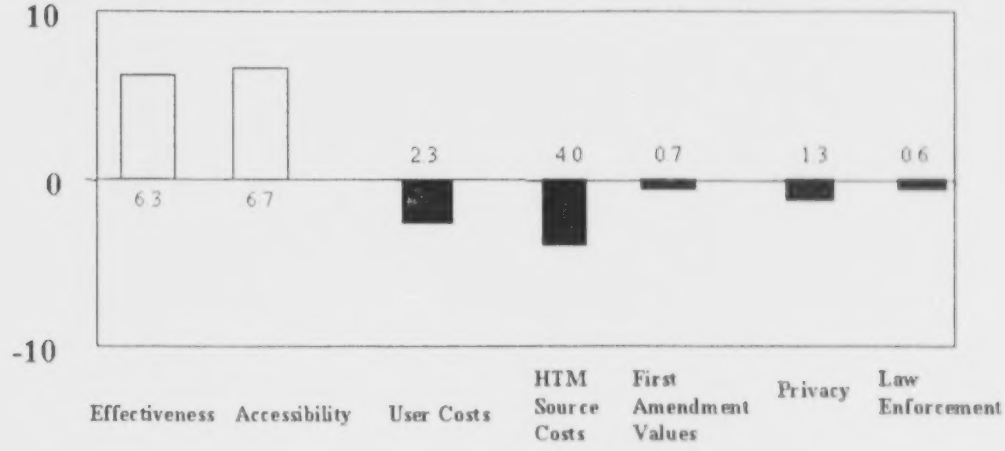
[9] ICANN (the Internet Corporation for Assigned Names and Numbers) was created in response to the call by the U.S. Dept. of Commerce, in their June 1998 "White Paper," for a "new not-for-profit corporation formed by private sector Internet stakeholders to administer policy for the Internet name and address system." It is responsible for technical management of the domain name system and for issues of management and administration of Internet names and numbers. Published sources indicate that ICANN has received applications to establish a .kids or similar top level domain.

there, and the concern about a "slippery slope" toward mandatory location in the gTLD.

- This approach raises the possibility of adverse effects on law enforcement, because creation of a "red light district" might serve as an attractive nuisance, and because incentives for law enforcement to prosecute unlawful material in the red light district might be reduced.

## 11. Establishment of a gTLD for non-harmful to minors content

Creation for voluntary use of a new top level domain (e.g., .kids) the use of which would be understood to signify that materials on web pages located in such domain (and email coming from such domain) would universally be considered suitable for minors of all ages -- and the existence of which would make it easy for browsers or ISPs to establish "green zone" features that point or accept only to such materials.

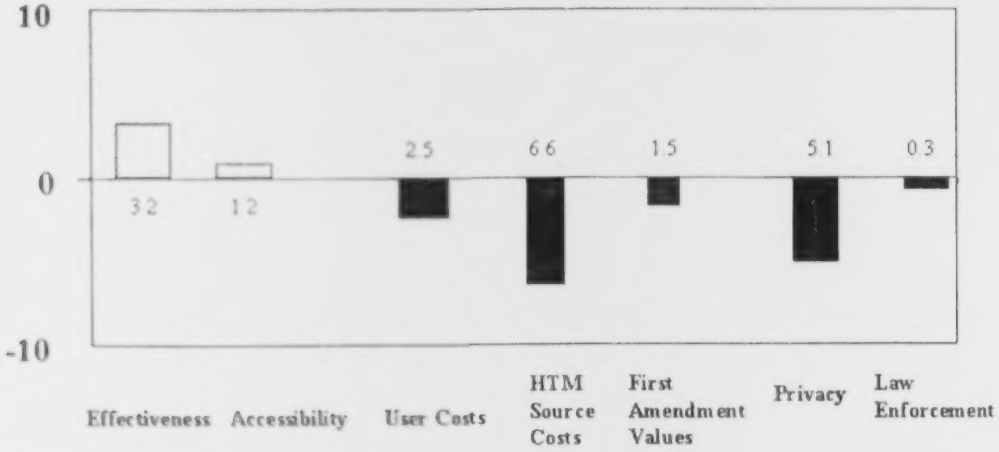



### Commentary

- This method is technologically feasible but such a domain does not currently exist. It requires that ICANN establish such a new top level domain. Again, the use of the domain system to implement policy raises questions. Alternatively, a lower level domain (such as .us.kids) could be established without the need for ICANN to take action.
- This approach could be an accessible and generally effective way to protect children from harmful to minors content. It would be more effective to the extent that children were restricted to such a zone. It would be more visible than mere establishment of multiple greenspaces or lists of child-appropriate sites. It would not, however, be effective at addressing content located in chat, newsgroups, or instant messaging.
- Costs to consumers and other end-users, to sources of harmful to minors content, to law enforcement, and to privacy interests are low.
- First Amendment concerns arise from fears that children, particularly older teens who are restricted to this zone, may be unable to access potentially informative and appropriate material.
- Creation of such a gTLD could have an adverse effect on law enforcement because of the risk that concentration of children's activities in this area could attract predators.

## 12. Establishment of a "green zone" or "red light zone" by means of allocation of a new set of IP numbers

Creation for voluntary use of a set of IP numbers (in the new IP version 6 protocol, which has not yet been widely implemented) the use of which would be understood to signify that materials on web pages on servers with such IP numbers (or email coming from such servers) would be either non-harmful to minors material or harmful to minors material, respectively. Any material not in such an IP number zone would be considered to be in a "gray zone" and not necessarily either harmful to minors or non-harmful to minors.



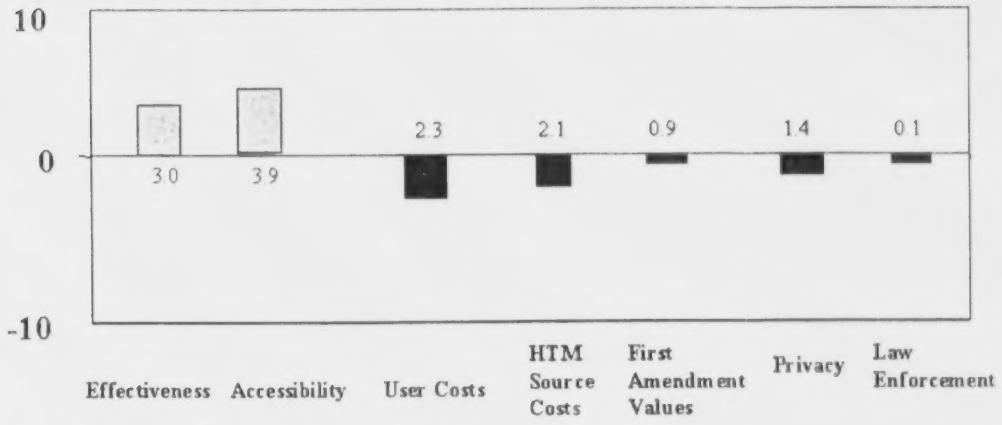

### Commentary

- This is a proposal for a system that does not currently exist. Technical difficulties involved in implementing this technology make effectiveness uncertain. Effectiveness would require substantial effort to attach content to specific IP numbers. This approach could potentially reduce flexibility and impede optimal network performance. It would not be effective at blocking access to chat, newsgroups, or instant messaging.
- Creation of a voluntary system dividing IP numbers could be the first step toward a mandatory division of IP numbers, which raises significant First Amendment concerns.
- This approach would impose significant costs on content sources, because it would require publishers to redesign hardware and allocate content between appropriate IP numbers.
- This approach would have little adverse effect on privacy or law enforcement.

## F. Other technologies or methods

### 13. Hotlines

Creation of facilities for easy reporting of problems to the parties who can address them, either online or via telephone. Such hotlines would bring problems to the attention of both relevant government authorities and private sector groups that can act in response to reported problems. Activity levels in aggregate and general nature of complaints would be made public.

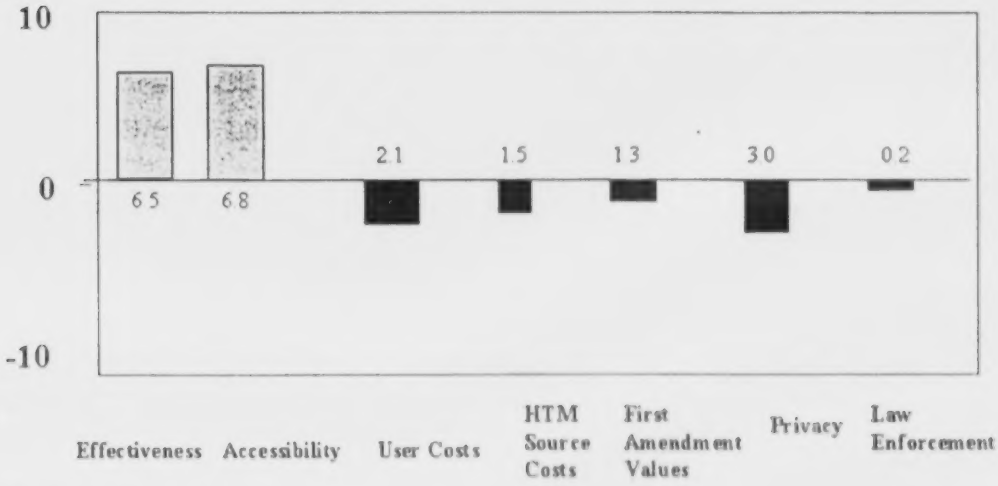



### Commentary

- Some service providers and law enforcement agencies currently operate hotlines.
- While hotlines do not directly block access to harmful to minors materials, they can be an integral part of an effective child-protection effort.
- Hotlines would increase visibility and information regarding the extent of problems concerning the exploitation of children, both for public and governmental use. High user costs reflect the fact that consumers ultimately bear the costs of hotlines, which can be substantial.
- Hotlines have little or no adverse effect on privacy and First Amendment values.
- The effect on law enforcement could be both positive and negative. Because of increased reporting, more information about harmful to minors material would be available to law enforcement. At the same time, law enforcement might receive more baseless reports.

## 14. Greenspaces

The voluntary creation of lists of materials determined to be appropriate for children and provision, via a browser or an online service or server filters, of an environment that allows children to go to or receive only such materials.

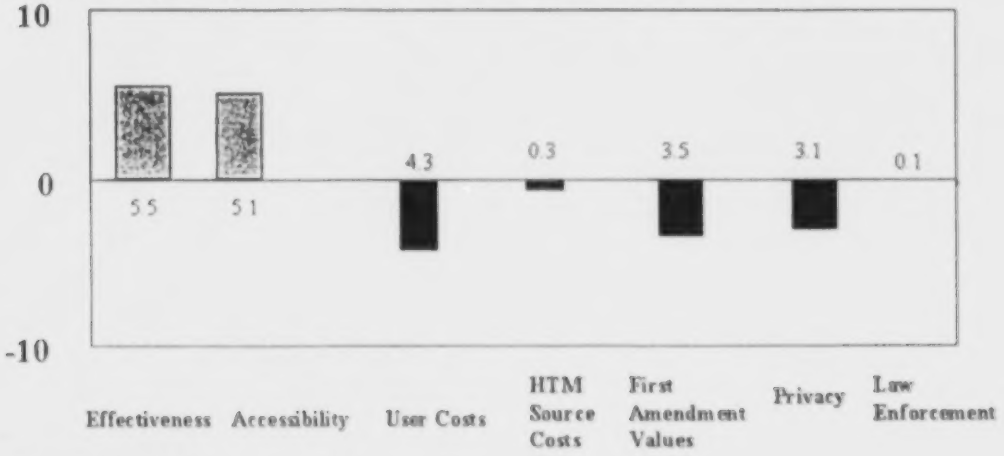



### Commentary

- Numerous greenspaces exist now, although many of them do not enjoy a high level of public awareness. Greenspaces may be very effective when they are readily accessible to children and when parents are involved in assuring that children use these spaces exclusively. It is unclear whether they are effective at blocking access to chat, newsgroups, or instant messaging.
- Effectiveness at protecting older children is limited, because they are more likely to seek access to content outside of the "walled garden" of greenspaces.
- Some of these content sources are available for a fee and thus impose a cost on consumers and other end-users. They may also impose some cost on publishers or compilers of greenspaces.
- While greenspaces impose little adverse impact on privacy and on lawful adult speech, concerns about First Amendment values relate to children's inability to access appropriate materials not incorporated into a greenspace.

## 15. Monitoring and time-limiting technologies

Use (typically at the PC) of software that creates logs showing details of a child's online activities and, optionally, enforces rules regarding the amount of time that may be spent online. Such systems may track both web use and email and instant messaging activities. In analyzing this technology/method, the Commission will assume that the child is told that the monitoring is taking place and that only the parent has access to the resulting information.



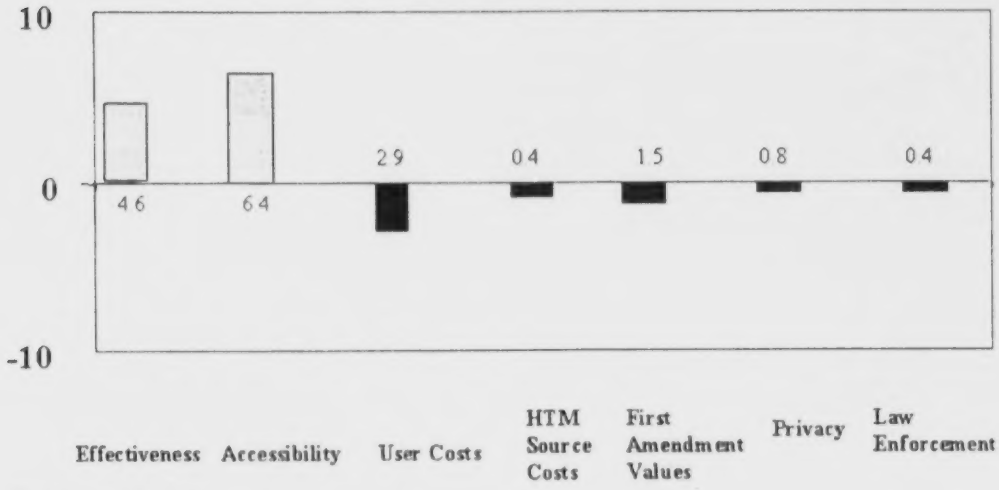

### Commentary

- These systems are available in the marketplace at this time. Some of them are sold as part of a filtering or blocking system. They work automatically and thus are not adversely affected by the constant changes in content available on the Internet.
- Monitoring and time-limiting technologies can be effective when used in the home because they influence children's activities and require involvement of parents. These technologies can be effective for email and other non-Web communication, and for access to global content.
- Monitoring and time-limiting technologies encourage greater parental involvement in the child's online experience; however, because a parent learns of activities only after the fact, effectiveness in reducing accidental access to harmful to minors materials may be limited.
- Use of these technologies requires some technical sophistication on the part of parents.
- Consumers and other end users absorb monetary and time costs to use these systems.
- The inability of teens to access appropriate informative materials without parental supervision and oversight is reflected in ratings regarding adverse effects on privacy and First Amendment values. Privacy concerns may be raised when this technology is used in schools and libraries.
- These technologies do not impose costs on providers of harmful to minors speech.

- The logs created by these technologies can be helpful to law enforcement in identifying predators.

## 16. Acceptable use policies/family contracts

Establishment by a parent or an institution (school or library) of rules regarding the types of materials that may be accessed. Typically, such policies would be enforced by means of denial of further access in the event of a violation. Such policies may or may not be accompanied by monitoring that would allow the parent or institution to detect violations.

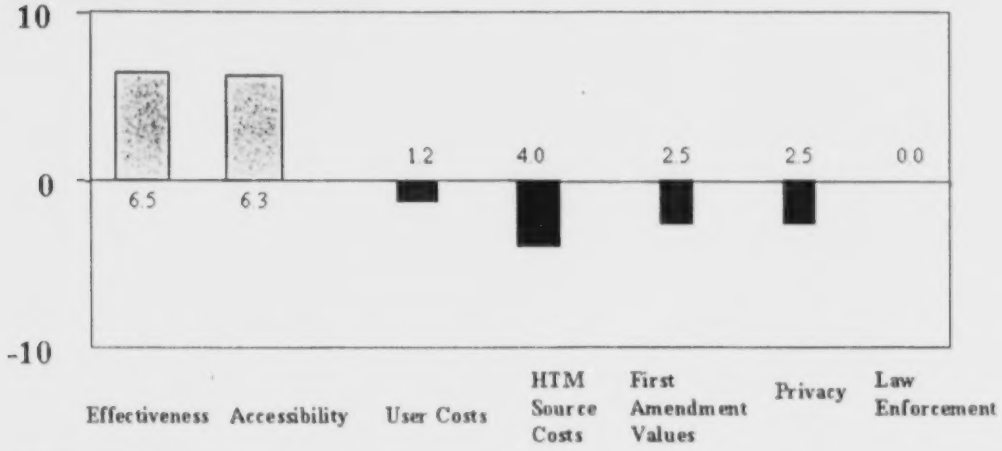



### Commentary

- Examples of many different kinds of acceptable use policies and family contracts are widely available on the Internet.
- Involvement of parents and institutions in expressly establishing guidelines through an acceptable use policy or family contract can have a significant positive impact on awareness and behavior, although they do not themselves directly reduce access by minors to harmful to minors material. While this approach can address the extent to which children seek out material, it is of less help in addressing accidental access or incoming spam.
- These approaches impose some cost on families and other caregivers because of the time commitment involved for active implementation and involvement.
- This approach imposes negligible costs on providers of harmful to minors material.
- When used in schools or libraries in conjunction with monitoring, this approach may raise privacy and First Amendment concerns.

## 17. Increased prosecution

Governmental expenditure (at federal, state and local levels) of more funds to investigate and prosecute online activities that are unlawful. While this "method" assumes a change in current governmental activity, the Commission will analyze its likely effectiveness (and potential adverse impacts) to provide a basis for its recommendations. The Commission will assume that US law could not practically be enforced against all content sources located in other countries with differing legal standards for content.

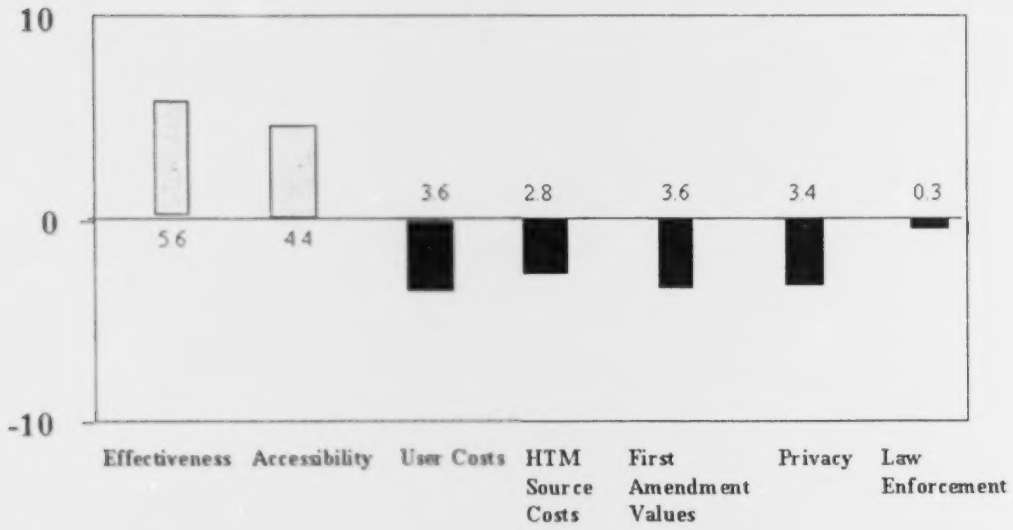



### Commentary

- This approach could be highly effective in reducing children's access to harmful to minors material because of its deterrent effect on publishers of illegal content. Targeted prosecution could show the US as an international leader, which might affect global enforceability over time. It is not clear that increased prosecution will have as significant an effect on content published outside the US, especially where the content might not be unlawful in the foreign country of origin.
- Costs to consumers of targeted prosecutions against clearly unlawful content would not be substantial. Sources of harmful to minors and lawful adult content could bear significant costs due to the need to assess the lawfulness of materials.
- Increased prosecution raises privacy risks because of law enforcement's increased efforts to obtain information about online activities. First Amendment concerns about increased prosecution relate to the chilling effect of investigation and decisions by lawful speakers to curtail speech to avoid risk of prosecution.

## 18. Real time Content Monitoring/Blocking

Use of real time monitoring methods to detect and block harmful to minors material sent via email, instant messaging, chat rooms and Usenet in addition to the web. Such monitoring assumes the ability to detect harmful to minors material in areas where filtering may not apply.




### Commentary

- Products meeting this description are available in the marketplace.
- This technique can apply to messages (e.g., real time chat) that cannot be filtered effectively with automated processes.
- To be effective, real time monitoring may require human involvement.
- The expense of human involvement may be substantial.
- To the extent that these products are more effective, potential impact on First Amendment values and costs to sources of harmful to minors content are increased due to the risk of over-blocking.

## III. RECOMMENDATIONS

After consideration of the record, the Commission concludes that the most effective current means of protecting children from content on the Internet harmful to minors include: aggressive efforts toward public education, consumer empowerment, increased resources for enforcement of existing laws, and greater use of existing technologies. Witness after witness testified that protection of children online requires more education, more technologies, heightened public awareness of existing technologies and better enforcement of existing laws.

Government at all levels and the Internet community must unite to provide broadly available education resources to families and caregivers. Voluntary methods and technologies to protect children must be developed, tested, evaluated and made readily available. Coupled with information to make these methods understandable and useful, these voluntary approaches provide powerful technologies for families. As we move forward, it is important that technologies to protect children reflect next-generation Internet systems and the convergence of old and new media. Finally, it is imperative that government allocate increased resources to law enforcement at the federal, state and local level for training, staffing and equipment so that existing laws against child pornography and obscenity are more effectively enforced.

Witnesses appearing before the COPA Commission testified that distribution over the Internet of obscene material, child pornography, and harmful to minors material continues to grow in a troubling manner. Law enforcement resources at the state and federal level have been focused nearly exclusively on child pornography and child stalking. We believe that an aggressive effort to address illegal, obscene material on the Internet will also address the presence of harmful to minors material.

The Internet's global nature presents law enforcement with an additional concern, because a substantial amount of obscene material, child pornography and harmful to minors material originates abroad. While issues of extradition, need for legal assistance from foreign law enforcement, and conflict of law issues make prosecution difficult, these problems have been addressed previously in the narcotics, fraud, and intellectual property areas. US leadership in this area may lead to models of international cooperation.

Public Education

- 1. **Recommendation: Government and the private sector should undertake a major education campaign to promote public awareness of technologies and methods available to protect children online.** Public education must be done in a sustainable manner that effectively reaches families both online and offline.

  - The campaign should stress the importance of involving caregivers in a child's online activity; the availability of both offline resources and one-click-away Internet technologies; access to child friendly sites; information about the range of technologies available to protect children; and information about testing and assessment of new technologies.

  - Public awareness efforts should include an online component, a targeted and cost-effective way to reach those who need help most – families on the Internet. Online initiatives can be a highly effective way to directly access information and technologies, providing families with one-stop shopping where they can get detailed information, report trouble, and be linked to technologies and resources so that they are only "one click away" from assistance.

  - Sellers of consumer PCs should be encouraged to stock filtering technologies, parental controls or other user empowerment technologies in a prominent place at the point of sale of consumer PCs to make such technologies easily available to consumers, and operating system sellers should be encouraged to bundle such technologies prominently within the operating systems.

  - Government at all levels should devote substantial resources as part of a public-private sector partnership to promote public awareness.

  - Public libraries, community centers, schools and PTA's would be essential components of this effort.

  - Resources should include information about access to law enforcement and child advocacy organizations.

- Government should provide block grants to states to create materials appropriate for Internet safety curricula. Materials for community and school publications, and libraries should be developed and distributed.

- **2. Recommendation: Government and Industry Should Effectively Promote Acceptable Use Policies.** Acceptable use policies refer to stated parameters for use of online systems. They are a non-technological technology or method for protecting children online. Government at all levels and industry should encourage parents and public institutions that offer access to online resources to adopt such policies. Just as we provide children with firm rules for crossing the street and guidelines for dealing with a variety of unfamiliar situations, we need to provide them with rules and guidelines to facilitate their online learning experiences as well as their safety.

- Acceptable use policies should be voluntarily implemented by public institutions that offer access to online resources. An acceptable use policy should disclose to parents what safeguards will be in place in the school and library setting that are designed to permit users to have educational experiences consistent with local or family values.

Consumer and Responsible Adult Empowerment

- **3. Recommendation: The Commission recommends allocation of resources for the independent evaluation of child protection technologies and to provide reports to the public about the capabilities of these technologies.** The current lack of information about how well technologies work, and lack of transparency about what they might block, is a major hurdle for their adoption by families or caregivers.

  - The Commission recommends that the private sector – industry, foundations, and public interest organizations - provide support for an independent, non-governmental testing facility for child-protection technologies. This facility would provide consumers with objective, well-researched information on the features, effectiveness, prices, search criteria, transparency, flexibility, and ease of use of various technologies.

- **4. Recommendation: The Commission recommends that industry take steps to improve child protection mechanisms, and make them more accessible online.**

  - Industry should improve filtering and blocking technologies, monitoring technologies, and child-safe "greenspaces." We support fully family and responsible adult decisions to use these Internet technologies.

  - Protective technologies, which feature strong visibility and easy implementation, have unusually high use levels. Service providers should make protective technologies more accessible and easier to use.

  - In addition, browsers, portals, and popular web sites could display parental control links in prominent locations. This is a low-cost, user-friendly method for bringing these resources to the attention of families and responsible adults.

- **5. Recommendation: The Commission encourages a broad, national, private sector conversation on the development of next-generation systems for labeling, rating, and identifying content reflecting the convergence of old and new media.**

  - The Commission has determined that rating and labeling may have positive synergistic effects on other technologies, such as filtering. The use of such systems could have a significant impact on consumer empowerment. This dialogue must consider the significant impacts on free speech and consumer privacy.

  - Recent advances in metadata may facilitate the implementation of such a rating and labeling system.

- **6. Recommendation: Government should encourage the use of technology in efforts to make children's experience of the Internet safe and useful.**

  - No particular technology or method provides a perfect solution, but when used in conjunction with education, acceptable use policies and adult

supervision, many technologies can provide improved safety from inadvertent access from harmful to minors materials.

Law Enforcement

- 7. **Recommendation: Government at all levels should fund, with significant new money, aggressive programs to investigate, prosecute, and report violations of federal and state obscenity laws, including efforts that emphasize the protection of children from accessing materials illegal under current state and federal obscenity law.** Specifically, the Commission recommends that Government at all levels fund aggressive programs to investigate and prosecute violations of obscenity laws.

  - This prosecution effort should include an emphasis on minimizing access by children to obscene material.

  - Significant new money should be appropriated to this effort to allow the investigation and prosecution of obscenity, child pornography and exploitation; train law enforcement officers, especially forensic investigators and examiners; and retain technical experts by increasing the ability of government to pay competitive salaries and benefits.

  - This investigation and prosecution program should supplement the Government's existing effort to investigate and prosecute child sexual exploitation, sexual abuse, and child pornography.

  - Such a program should be of sufficient magnitude to deter effectively illegal activity on the Internet.

- 8. **Recommendation: The Commission recommends that state and federal law enforcement make available a list, without images, of Usenet newsgroups, IP addresses, World Wide Web sites or other Internet sources that have been found to contain child pornography or where convictions have been obtained involving obscene material.** This information may be used to identify obscene materials or child pornography under the control of the ISP or content provider. The Commission recognizes

that, consistent with this recommendation, law enforcement will take appropriate steps to limit dissemination of this information to those entities that have a legitimate purpose for accessing such information. Use of this list must remain voluntary.

- 9. **Recommendation: The Commission recommends that Federal agencies, pursuant to further Congressional rulemaking authority as needed, consider greater enforcement and possibly rulemaking to discourage deceptive or unfair practices that entice children to view obscene materials, including the practices of "mouse trapping" and deceptive meta-tagging.**

  - Prosecution should focus on major producers, distributors, and sellers of obscene material that use fraudulent or misleading methods to market their material to children.

- 10. **Recommendation: Government should provide new money to address international aspects of Internet crime, including obscenity and child pornography.**

  - The Federal Government should review and seek to amend or negotiate new international agreements to address extradition and the gathering of evidence in cases involving international distribution of obscenity and child pornography over the Internet.

  - Provide new and substantial funding to enable investigation and prosecution of international obscenity and child pornography distributors and producers that use the Internet to distribute or sell said material

  - Congress should review federal rules of evidence and procedure to determine its sufficiency to deal with international investigations and prosecutions and make any necessary changes

Internet Service Provider Industry Self-Regulation

- 11. **Recommendation: The Commission urges the ISP industry to voluntarily undertake "best practices" to protect minors.** These practices should include:

- Voluntarily providing, offering, or enabling user empowerment technologies to assist end-users to protect children from material that is harmful to minors.

- Providing that ISPs, when made aware of violations of best practices, will address them in a timely manner.

- Stating that ISPs reserve the right to take action in good faith to restrict availability of material that violates best practices.

- Increasing awareness among ISPs and promoting timely implementation of their legal obligations to remove child pornography hosted on their own servers when notified of its presence.

- Voluntarily cooperating with local, state, federal, and international authorities in the investigation of crimes involving the use of their service, to the extent practical and lawful.

Adult Industry Self-Regulation

- **12. Recommendation: The Online Commercial Adult Industry Should Voluntarily Take Steps To Restrict Minors' Ready Access to Adult Content.** Representatives of the commercial online adult content industry testified to their willingness to take voluntary steps to reduce ready access to online commercial adult content by children. Self-regulatory steps could restrict children's access to commercial online adult content and thus address a substantial portion of the concerns surrounding such materials.

  - These efforts should call on members to provide that the public front pages of commercial adult content sites will not contain explicit graphics or text, but be limited to material sufficient to make clear that the site contains sexual material. Teaser pages should be located only beyond the front, public page.

  - These efforts should call on members to use the most effective currently available technologies for verifying age, the further development and use

of which should be a priority.

- Self-labeling is potentially among the most effective means of empowering parents to limit access to harmful to minors material, especially in concert with other technologies and methods such as filtering. This industry should pursue efforts to encourage web sites to self-label and should provide incentives for them to do so.

- These efforts should call on members to avoid use of metatags that result in their sites being selected by search engines in response to searches seeking information of a nonsexual nature, or in the posting of search engine responses containing sexually-explicit text or graphics. Children entering innocent search requests, or accidentally mis-typing a request, should not be presented unexpectedly with lurid text and graphics. Search engine responses should simply reflect that the content of pages responsive to the request contain sexual material.

- These efforts should call on members to comply with federal and state laws applicable to unsolicited commercial email, and not to use mass, unsolicited emails likely to include addresses available to children to promote adult content. Commercial email promoting adult sites should not contain links directly to adult content. Any commercial email should be targeted only to adults and should contain a prominent disclosure that it promotes sexually explicit sites.

## IV. AFFIRMATIVE DEFENSES

The Congressional charge to the Commission states that "[t]he Commission shall conduct a study to identify technological or other methods that (A) will help reduce access by minors to material that is harmful to minors on the Internet; and (B) may meet the requirements for use as affirmative defenses for purposes of section 231(c)." Section 231(c), in turn, describes these requirements in terms of actions taken to restrict access by minors to material that is harmful to minors by means of "any reasonable measures that are feasible under available technology." Section 231(a) and (b) already recognize use of credit card and other age verification systems as affirmative defenses.

The Commission discussed whether and how to respond to the Congressional charge in Section B quoted above, in light of the fact that the COPA statute has now been preliminarily enjoined as unconstitutional. The Commission agreed that the question presented to it is not whether or not a particular technology or method should or should not be considered an affirmative defense, much less whether any statute should be found constitutional or unconstitutional. We interpret the question presented to the Commission in Section B as asking whether there are any feasible technologies or methods that are currently available and that may constitute "reasonable measures" to restrict access by minors to harmful to minors materials.

The Commission studied many different technologies and methods that may be used to restrict access by minors to harmful to minors materials. Some technologies did not meet all the statutory requirements because they are not feasible or are not currently available. We determined, however, that some of the technologies we analyzed, for example first party labeling, may become "reasonable" means of preventing child access to harmful to minors material when such technologies become more widely adopted in the marketplace. We did not have the time or resources, however, to conduct a detailed inquiry into the "reasonableness" of the use of any particular technology in the hypothetical context of an assertion of an affirmative defense under COPA. Because of the limitations on its study, the Commission did not conclude that any particular technology "may meet the requirements for use as affirmative defenses for purposes of section 231(c)."

## V. PROPOSED FUTURE WORK

The Commission is concerned that its lack of funding and short timetable has limited the inquiry in which it has been able to engage. We anticipate that, with additional resources and an extension of the statutorily allotted time for submission of this report, the Commission would have undertaken the following efforts to provide the Congress with a more in-depth and detailed report:

1. *Engage in a more robust analysis of technologies and methods.*

- Conduct a more in-depth examination of individual technologies. This examination could include convening additional hearings on technologies

about which we received insufficient testimony and observing technology demonstrations.

- Present our recommendations for review by a panel of technical experts.

- Investigate new technologies that came to the Commission's attention.

- Clarify and break out the criteria and assumptions for evaluation of technologies and methods to allow the Commission to make more meaningful and specific assessments of individual technologies. Such an approach would allow the Commission to examine the distinct Constitutional and privacy impact, as well as the usefulness of these technologies in the home, school and libraries.

2. *Investigate the criteria and explore models for an independent testing lab that would provide consistent, reliable evaluation of technologies and provide an optimal service to the industry and consumers.*

3. *Solicit input from additional operators of filtering and monitoring systems.*

While this additional effort would have been desirable, it does not detract from the fact that the information gathered by the Commission was significant in quality and quantity, and provides an ample basis for our conclusions and recommendations.

## VI. CONCLUSION

The Commission appreciates the opportunity to have served the Congress of the United States by studying technologies and methods designed to reduce access by minors to "harmful to minors" material on the Internet. We respectfully submit this document as our final Report.

## APPENDIX
## TABLE OF CONTENTS

**An electronic version of the report's appendix, including a detailed index of documents that were submitted to the Commission, are available on the COPA Commission web site at www.copacommission.org.**

Appendices to COPA Commission Report

**A. Commission Overview**

1. Scope and Timeline
2. Original Statute
3. Amended Statute
4. Technologies and Methods
5. Biographies of the Commissioners

**B. Commission Finances**

1. Report on Commission Finances

**C. Commission Meetings**

1. Meeting, March 7, 2000
2. Meeting, April 28, 2000
3. Meeting, June 9, 2000
4. Meeting, July 21, 2000
5. Meeting, August 4, 2000
6. Report Drafting Meeting, September 18-19, 2000
7. Report Drafting Meeting, October 4-5, 2000

**D. Materials Submitted to the Commission**

1. Hearing 1, June 8-9, 2000
2. Hearing 2, July 20-21, 2000
3. Hearing 3, August 3-4, 2000
4. Research Papers and Reports
5. Correspondence

**E. Compilation of Matrices on Filtering, Labeling, and Rating Technologies**

**F. Commission Responses to Questionnaire**
The Commissioner's individual responses to the questionnaire are available on the COPA Commission's web site at www.copacommission.org

**G. Catalog of Drawer Files**
A detailed index of all materials submitted to the commission in non-electronic format such as books, software programs, and handouts. Also includes VHS tape recordings of hearings and transcripts.

# PERSONAL STATEMENTS OF COPA COMMISSIONERS

COMPANION VOLUME TO
THE COMMISSION ON ONLINE
CHILD PROTECTION (COPA)
REPORT TO CONGRESS

October 20, 2000

Donald N. Telage
Executive Advisor for Global Internet Strategy
Network Solutions Inc.
Chairman, Commission on Online Child Protection

I am deeply proud to have served as the Chairman of this distinguished Commission. The Commission has struggled with a difficult and multi-dimensional problem and has emerged with thoughtful and constructive unanimous recommendations that will serve as a blueprint for future action. Each Commissioner has approached the hard work of the Commission with enormous seriousness, collegiality, good will, high energy, and intelligent engagement. It has been, for me, a moving experience to serve with these Commissioners, and I am grateful to have been given the opportunity to facilitate in the Commission's efforts.

The Commission's recommendations not only reflect the will of the Commission but also represent the distillation of an enormous amount of material with which the Commission was presented over the last six months. Our hearings, held in Washington, D.C., Richmond, Virginia, and San Jose, California, were instructive -- there was a great deal to learn about the various technologies and methods studied by the Commission. Commissioners closely questioned witnesses, brought to bear their own rich expertise, and most importantly focused intensely on the questions presented to the Commission by Congress. Our conversations were always constructive, and often animated, and yet a spirit of public service punctuated every meeting.

This discussion is clearly not over. The work of this Commission shows that people holding widely-divergent political points of view can reach consensus as to the strengths and weaknesses of technologies and methods that may help protect America's children from accessing "harmful to minors" material on the Internet. It is my hope that this conversation, held so effectively and with such genuine thoughtfulness among the Commissioners, will continue in many places and among many different groups. The Commission has recommended that the online industry in general have a conversation about the necessity for and efficacy of labeling and rating systems (which may have significant synergistic effects with other technologies), and that the adult content industry in particular have a conversation about regulating itself. These conversations are fundamentally

important, and all of us will be well served by continuing constructive exchanges of ideas in the same spirit in which the Commission operated.

I want to take this opportunity to thank my chief of staff, Kristin Litterst of Dittus Communications and her team for their dedication. She was the backbone of this Commission and I owe her an immense debt of gratitude. I would also like to express my gratitude to Network Solutions, Inc for its support of Ms. Litterst and her staff. Finally, I wish to thank David Johnson and Susan Crawford, my counsel, of Wilmer, Cutler & Pickering, for their never-ending wisdom and the river of creative ideas they supplied to the Commission. The efforts of Mr. Johnson and Ms. Crawford were pro bono contributions to me. This support was facilitated by Mr. Lloyd Cutler, founder of that firm, resulting from our discussions of the importance of the COPA challenge.

In the pages that follow, each COPA Commissioner has been afforded an opportunity to provide their individual personal view of the work of this Commission and the position they would have taken if acting alone. The range of views these statements reflect render our unanimous recommendations all the more remarkable.

# Joint Statement of Government Representatives to the COPA Commission[1]

As children's Internet access has increased, so too have concerns that they have positive, safe online experiences. Children are shielded from commercial pornography in the real world of homes, schools, libraries, and neighborhoods. In neighborhood convenience stores and other areas that children frequent, for example, pornographic magazines are shielded from public view behind brown wrappers and located on the higher shelves, and not sold to minors; television rules limit programming containing indecent adult material to late evening hours.

Children are entitled to an analogous level of protection online. Often, they do not have this. Innocent search requests turn up lurid descriptions of pornographic sites that can be accessed via a mouse-click. Unsolicited email promotes access to this material. At best, these experiences are discomforting and unwelcome. The children who testified at the COPA hearings voiced their unease with the intruding presence of online pornography. Moreover, children may be lured to Web sites where they do not belong.

The Child Online Protection Commission was established by Congress to look at tools and methods to protect children from harmful to minors materials online. The Administration believes that the work of the Commission is vitally important in this effort. Acting under a tight deadline and difficult circumstances, the Commission has developed an extensive and valuable record regarding the available child-protective tools and methods. Each member contributed his or her expertise and demonstrated objectivity in considering the wide range of evidence presented at the hearings. The Commission as a whole and the individual Commissioners deserve high praise for their efforts.

The Administration has long supported an industry-led, self-regulatory approach to address these concerns. First, it has encouraged industry and nonprofit organizations to develop and provide ready access to child-friendly, quality content on the Internet and to develop technological tools that help

---

[1] **We would like to acknowledge the following staff members, who assisted our work on the COPA Commission: Janet M. Evans, Federal Trade Commission; Sallianne Fortunato and Kelly Levy, National Telecommunications and Information Administration, Department of Commerce; Janis Kockritz and Hemanshu Nigam, Department of Justice.**

parents and guardians protect children from material they consider harmful or inappropriate. Second, it has encouraged public institutions offering Internet access to adopt "acceptable use" policies that offer parents a reasonable assurance that schools and libraries have safeguards in place to permit users to have educational experiences consistent with their local values. Third, it has strongly supported the enforcement of existing laws that prohibit the distribution of child pornography, distribution of obscene material, and use of the Internet to entice children away from the safety of their homes. Through projects like the FBI's Innocent Images Project, which includes representatives of the Postal Inspection Service and the U.S. Customs Service, the U.S. Government is continuing to combat the use of the Internet to traffic in child pornography and to stalk children for illegal sexual activity. Additionally, the Administration has actively advanced policy regarding Internet content, both in bilateral discussions and multilateral meetings with foreign governments. Bilateral agreements with foreign governments have emphasized the importance of filtering technologies rather than the use of government censorship to protect minors from accessing inappropriate material on the Internet.

The record of the COPA hearings makes clear that significant efforts have been made to respond to this challenge of protecting children online. The child-protective tools and methods available to date permit parents, teachers, and librarians to provide children with some level of protection on the Internet. As currently configured, these tools provide a limited level of safety and are likely to reduce child access to online pornography and other harmful to minors materials. Still, it is clear that they are not up to the task of providing full protection. Indeed, no one approach or tool, alone, is likely to provide children with protection from such material. Instead, government and industry need to work together to devise an improved "safety net" of protections -- coupling improved technology with new self-regulatory standards -- to reduce children's exposure to commercial pornography and other sexually explicit materials online.

The Administration looks forward to working with lawmakers and industry on improving protections for children online. During the COPA hearings, we identified efforts that government and industry could take to increase protection of children online; these proposals are described below. We are pleased that the Commission endorsed many of these suggestions, addressing them in its recommendations. If the COPA Commission's recommendations are

implemented, we believe that they will result in meaningfully increased protection of children online.

**Local, State, and Federal Governments Should Increase Enforcement of Laws Prohibiting the Distribution of Child Pornography, the Intentional Distribution of Obscene Materials to Minors, and the Use of the Internet to Entice Children for Illegal Sexual Activity.** The Internet has become the online equivalent of the proverbial "playground" frequented by predators seeking child victims. Law enforcement must continue to investigate and prosecute instances of child exploitation via the Internet.

- Multi-agency task forces, such as the Internet Crimes Against Children Task Forces sponsored by the Office of Juvenile Justice and Delinquency Prevention, work together effectively to enforce state and federal crimes against children.

- Multi-disciplinary centers for the investigation of computer crimes, such as the U.S. Customs Service's Cyber Smuggling Center, bring together the expertise of online investigators and computer analysts to combat the use of the Internet to commit a myriad of crimes, including the distribution of child pornography.

- The FBI is expanding and will continue to expand its "innocent images" project by creating regional "franchises" to aggressively target child pornographers and predators wherever they are found.

- Continued funding is necessary to cover the costs of these pro-active online projects and to train new agents on the techniques of online investigations.

**Browsers Should Feature A "Parental Control" Button In a Prominent Location.** This feature would increase accessibility of child-protective tools and methods. This is a low- cost, user-friendly method for bringing these tools to parents' attention.

- The Administration strongly supports one-click-away type of tools that can provide parents easy online access to tools and information about keeping their children safe online. The Administration has also been a strong supporter of the public interest group/industry-led initiative "Get Net Wise," an easy-to-access online resource for parents to help them keep their children safe online.

by providing information on Internet safety tips, consumer content filtering products, law enforcement contacts, and guides to quality educational and age-appropriate online content.

**The Online Commercial Pornography Industry Should Voluntarily Adopt Standards That Restrict Ready Access to Pornography**. In addition to whatever effective legal protections can be fashioned, it is clear that the online commercial pornography industry itself can and should be doing more to protect children from online access to their products. This industry has stated its willingness to engage in self-regulation. It should adopt standards to reduce ready access to online commercial pornography by children.

- These standards should require use of the most effective available technology for verifying age. While genuine age verification technology is not yet available, its development must be a priority. Until such time, industry should require credit card verification or other adult identifier confirmation to access these sites.

**The Online Commercial Pornography Industry and Search Engine Operators Should Voluntarily Adopt Standards To Reduce Intrusiveness of Pornography.** These industries should adopt a cyberspace equivalent of a "plain brown wrapper" for commercial online pornographic material.

- The public front pages of commercial pornographic sites should not contain explicit graphics or text. They should be limited to material sufficient to make clear that the site contains sexual material. Teaser pages should be located only beyond the front, public page.

- Children entering innocent search requests, or accidentally mistyping a request, should not be unexpectedly presented with lurid text and graphics. Internet searches seeking information of a non-sexual nature should not receive responses containing sexual text or graphics. Return links should simply reflect that the content of linked pages responsive to the request contain sexual material.

**Industry Should Improve Available Technological Protections, Including Filtering and Blocking Technologies, Monitoring Technologies, and Child-safe "Green Spaces."**

- We fully support community decisions to use Internet blocking and filtering technology. These protections should be made more accessible and easier to use.

- Only a third of parents now avail themselves of these tools. Low use levels are likely due to lack of familiarity and difficulty of use. The record shows that one company's parental controls, which feature strong visibility and easy implementation, have unusually high use levels.

- Other service providers should make parental controls easy to access via links from their home pages. Protective technologies also should take steps to make their products easier to use.

- The COPA Commission found little objective information about the actual effectiveness of the technologies at blocking access to pornography. The Administration supports objective third party testing of the various filtering and blocking products, in order that they may compete on the basis of efficacy and thus achieve more widespread use.

**The Online Industry Should Provide More Support to Rating Systems.** Substantial effort has been committed to ratings systems but they have not yet reached critical mass.

- Large sites should voluntarily participate in ratings efforts, as they can be used to facilitate parental choice.

**Government and Industry Should Promote Acceptable Use Policies.** Acceptable use policies are a non-technological tool for protecting children online. The Administration encourages parents and public institutions that offer access to online resources, including the Internet, to adopt such policies. Just as we provide children with firm rules for crossing the street and guidelines for dealing with a variety of unfamiliar situations, we need to provide them with rules and guidelines to facilitate their online learning experiences as well as their safety.

- The Administration has supported legislation that requires that any school or library that receives federal e-rate funds must have an acceptable use policy in place before such funds are awarded to them.

- The Administration encourages use of acceptable use policies by all public institutions that offer access to online resources, including the Internet. An acceptable use policy should, while being sensitive to local needs and concerns, offer reasonable assurances to parents that safeguards will be in place in the school and library setting that permit users to have educational experiences consistent with their values.

**Conclusion.** The COPA Commission completed a complex task in a short amount of time under difficult circumstances. Its Report will provide significant assistance to industry and government alike as we continue to grapple with the difficult issue of protecting children online while ensuring the broadest possible flow of information.

Signed:

C. Lee Peeler,
Associate Director, Division of Advertising Practices, Federal Trade Commission

Michael Horowitz,
Chief of Staff for the Assistant Attorney General to the Criminal Division, Department of Justice

Gregory L. Rohde
Assistant Secretary for Communications and Information and Administrator, National Telecommunications and Information Administration, Department of Commerce

Commissioner Stephen Balkam
Executive Director
Internet Content Rating Association

The Internet changes everything. It upsets our notions of how things should be, how countries should be governed, how companies should be run, how teachers teach and children learn. It mixes up our conceptual framework of what we think we know about the world, about each other and about ourselves. It is liberating, exciting, challenging and terrifying all at the same time. It is technology as a social force and it is instantaneous and it is everywhere. No wonder the Chinese authorities want to keep it from its people.

While the Internet has and continues to grow at an exponential rate, we remain witnesses to the first faltering steps of a phenomenon that is still in its infancy. To a majority of the world's people, the Internet remains mysterious, forbidding, incomprehensible and frightening. The greatest inhibitor to the continued growth of this new medium is fear. And when you ask people what they are most frightened of, invariably they return the top three concerns of porn, privacy and security. While the COPA Commission heard testimony that touched on the issues of personal privacy and numerous security issues, we focused on the issue of material deemed "harmful to minors". The US Congress asked us to recommend constitutionally acceptable remedies that would help shield children from pornographic images, while continuing to respect the rights of adults to access this type of material. I believe our multi-faceted approach of public education, increased prosecutions, the further development of filtering tools, the promotion of self-labelling and self-regulatory regimes within both the ISP and adult industries, is a remarkably comprehensive and dynamically balanced approach. I applaud my fellow Commissioners and their staff for bringing us to these conclusions.

It has not been easy. We had little time and even less money. We took our hearings out on the road which added to the challenge while reaping greater rewards in the quality, range and depth of the testimonies. We are a disparate group from a broad range of political, moral and personal perspectives. This diversity contributed to the challenge of reaching consensus on so many hotly disputed issues. It is a testimony to our

Chairman, Don Telage, that we remained so cohesive and productive as a group.

Doubts remain, however, on how best to further what we have begun with our findings and recommendations. It became obvious to me during the Third Hearing in San Jose that a similar Commission was needed to address the same issues on an international basis. Although the United States has long lead the Internet revolution, other countries and regions of the world have fast caught up and are taking this medium into new and uncharted territory. I am thinking in particular about wireless applications and the convergence of media into Internet appliances. The United States must share what it has learnt while remaining open and receptive to other approaches emerging in Europe, the Asia Pacific and beyond. This is not exclusively a US problem, nor will an exclusively US range of remedies work in this the most interlinked and international media the world has ever known. New governmental, organisational and association models will have to be found to bridge the linguistic, cultural and political differences that bear on this issue when it is addressed at a global level. The ICANN experience is a recent example of this new world and it can be a tough and painful road.

Finally, we need to more vigorously spread the gospel of industry responsibility and consumer empowerment. The myriad of companies, concerns and individuals that make up the "Internet industry", while resisting government legislation, must see that it is in their own commercial interest to participate, fund and develop self-regulatory efforts in this area. Similarly, parents, caregivers and other concerned adults will need to invest some time and energy in getting to know what tools are available to protect their children from the worst of the web. Industry must make those tools easy to find and easy to use. Parents must be encouraged, educated and persuaded to use them. It is neither practical nor desirable for a governmental censor to pick and choose what a child will experience on the Internet. While government has a reduced role to play in this area, it can legitimately keep up the pressure on Industry to respond to the legitimate concerns of consumers. Government must finesse the art of carrot and stick and it must find new ways to do this in a global environment.

Commissioner John C. Bastian
CEO, Security Software Systems

The rapid growth and popularity of the Internet has made it an indispensable vehicle for commerce, information and communication. With a vast interactive audience, a wide diversity of content is available to any Internet user. Unrestricted access provides the ultimate diversity in information, culture, art, music and sex.

Harmful to Minors (HTM) content is a large, diverse part of the Internet. Hundreds of thousands of explicit web sites exist with millions of pages of HTM material are easily accessed by a few clicks of a mouse. Marketing strategies of these "sex" businesses vary widely from simple real-world advertising to unsolicited explicit email spams.

Commissioners heard testimony from a wide diversity of organizations, technology vendors and individuals who all represented their perspective and information succinctly. However, I feel we have only opened the door on many issues and because of time and resource limitations, not fully explored important facets of our investigations.

I believe an acronym is appropriate to express the diversity a solution may entail.

The ALERT Equation

Awareness, Law enforcement, Education, Responsibility and Technology all have a part to play in the protection equation. As we all learned. a single solution, or magic bullet is not a reality.

Awareness

A sensible approach is necessary to inform caregivers and young net citizens of the dangers of unrestricted on-line access but balanced with the benefits and responsibilities that go with its use. Awareness is not just identifying the problem, it must encompass solutions. Throughout history, society has paid a cost for technological advances. The major difference with the "on-line" generation is the simple fact that children are the early adopters and can have a higher degree of technological knowledge than the adult caregiver. This not an "out of sight, out of mind" problem, awareness is a key element. Harmful to minors material, designed for an adult audience often is easily

accessible by a child. Access can be accidental or intentional, but the result is the same.

Law Enforcement

Even though the report centers on HTM content, a serious problem exists for children in the form of sexual predators and pedophiles. Law enforcement witnesses attested to the dramatic rise in child molestations arising from open or unmonitored Internet communication pathways. Chat rooms, e-mail and Instant Messengers have given a new channel for predators and pedophiles to solicit children.

Current laws need to be fully enforced by well trained, web savvy officers and prosecutors.

Education

Schools, Libraries, Government and Industry must initiate a major educational campaign to inform the public of protective technologies and methods available to protect children online.

As caregivers, we all need to be involved and educated in the process of protecting our children to assure a positive experience for our youth.

Responsibility

Partnerships need to be established between Government and the Internet community to fund programs designed to; educate caregivers, promote public awareness, develop new protective and investigative tools. Federal, State and Local Law Enforcement needs adequate funding to train and add staff.

The adult industry has to take responsibility as well. Pornographic site operators fail to understand that even "teaser page" or "mouse trapping" marketing tactics are detrimental to children. We cannot assume pornographers will ever become "good" internet citizens as some witnesses purported. Even explicit sites touting protective technologies still place this technology behind the teasers. Caregivers also have the responsibility to learn the facts and know what the child is doing on-line.

Technology

The real-time nature of the Internet allows site content to be changed at anytime. Because of this fact, technology designed to protect children from HTM materials faces significant challenges. Chat rooms, E-mail and Instant Messaging are additional challenges for technology. As testimony indicated,

there is a real need for a credible independent "benchmarking" organization to evaluate marketplace protective tools for effectiveness and proper application. We found that "one size fits all" is not the reality. Protective technologies are as diverse as their clients.

Challenges

Today's youth face a multitude of challenges regarding technology that many adult caregivers cannot fully understand. We, as a society, face the challenge of protecting our children from inappropriate content and communications from a new media that has a unique character.

In recent history, the dominance the U.S. experienced in the Internet community is being diminished by fast adoption in other countries. Soon half the content on the web will be from foreign sources. This provides multiple challenges for law enforcement, legislators, child protection technology vendors and more importantly, children.

I would like to thank all my fellow commissioners and the support staff for their dedication to this commission. Additionally, I would like to thank all the witnesses for their insight and commitment.

Commissioner Jerry Berman
Center for Democracy and Technology

The Center for Democracy and Technology participated in the work of this Commission with two goals in mind. First, CDT sought to empower parents to protect children online in a manner consistent with their own values as individual families. Second, CDT sought to protect First Amendment values on the Internet – a democratizing medium that expands the power of citizens to engage in speech in unprecedented ways.

The recommendations of this report endorse the policy CDT pursued. Acknowledging the unique, global character of the Internet, the Commission concludes that new laws would not only be Constitutionally dubious, they would not effectively limit children's access to inappropriate materials. The Commission instead finds that empowering families to guide their children's Internet use is the only feasible way to protect children online while preserving First Amendment values. The Commission cites public education, user empowerment and enforcement of existing laws against obscenity and child pornography as the most effective means to assure the safety of children online. To realize the full potential of these approaches to protecting children, the Commission's recommendations call for a redoubled commitment of resources for further development and deployment of tools and educational materials.

**The Nature of the Internet and the Protection of Children**

The Commission On Online Child Protection has done what Congress has not – it has examined how to protect children online in ways consistent with the Internet's architecture and Constitutional requirements. The Commission reviewed testimony describing the global reach of the Internet, the decentralized nature of its architecture, and its ability to promote the speech of a wide range of speakers representing diverse values. The Commission rejects a legislative approach to protecting children not only because laws restricting distribution of or access to harmful to minors materials are Constitutionally suspect, but also because United States law cannot affect the flow of content originating in other countries and therefore cannot effectively protect children.

The Commission also considered whether any of the technologies and methods it reviewed could serve as an affirmative defense to a violation of the criminal provisions of the Child Online Protection Act. Keeping in mind the Internet's unique character, the Commission finds that none of the approaches could adequately serve as an affirmative defense in a manner respectful of the First Amendment.

Finally, the Commission rejects the creation of a top-level Internet domain for material harmful to minors. The Commission recognizes that such an approach could only succeed if mandated by law, and that such mandatory zoning would present serious First Amendment problems and chill protected speech.

## The Commission's Recommendations

The Commission recommends increased education for children and their families. Public education is a powerful tool to protect children and does not restrict protected speech. But to succeed, public education must be deployed with serious commitment and substantial resources. When we educate children at home and at school, we impart important values to them – we teach them to use seat belts, not to smoke, and to stay away from illicit drugs. Our message to children about safe activity online must be as clear and strong. Industry and government must also commit the resources necessary to promote widespread family awareness of the importance of protecting children online and the practical ways in which families can protect children.

The Commission recommends, and CDT concurs, that education must be coupled with empowerment tools. While monitoring and filtering technologies are available to parents, it is critical they be evaluated, assessed and tested, so that families know what tools are available to them, what they do, and how well they work. Information about these tools must be widely available, so that families have the information they need to make choices about their children's online experience that reflect their values.

Finally, recognizing that new laws against harmful to minors materials would not survive judicial scrutiny, the Commission urges Congress and law enforcement to focus on better enforcement of existing laws against obscenity and child pornography. These laws target unprotected speech and are clearly

Constitutional. Historically, enforcement of these laws online has suffered from insufficient funding. A renewed commitment to their robust enforcement and full funding can assure that children can safely take advantage of the positive resources the Internet offers.

## A Word of Thanks

It has been a pleasure to serve on this Commission. With no resources from the Congress, the Commission worked diligently and in good faith. This report reflects the effort of Commissioners representing diverse perspectives on the question of how best to protect children online. It is an example of how individuals holding a range of opinions can, through a thoughtful, deliberative process, find common ground.

The work of the Commission was facilitated by the tremendous effort of people who care about protecting children. I would like to thank the Chairman and my fellow Commissioners. I would also like to acknowledge the work of Dittus Communications, the contribution of the law offices of Wilmer, Cutler and Pickering, and the funding by companies who stepped in with resources when the Congress did not. Finally, I must thank Alan Davidson, Paula Bruening, and Rob Courtney of the Center for Democracy and Technology, whose efforts behind the scenes were critical to the success of this endeavor.

Commissioner Arthur H. DeRosier, Jr.
Rocky Mountain College

Participating in the Commission on Online Child Protection has been both frustrating and exhilarating. Nineteen original Commissioners were faced with an assignment without federal funding, and a timetable almost impossible to meet—seven months from meeting each other in Washington, D.C. in March, 2000 to an agenda, hearings, evaluation of myriad technologies and invited and non-invited reports, articles, and expressions of opinion, and, finally, the need to sift through it all finding nuggets worthy of consideration, and reaching recommendations worthy of the high calling felt by all of the Commission members in October 2000. To my knowledge, no investigating and recommending body has had more potholes to avoid, and no group with whom I have ever been associated worked harder or smarter for the public good than did the COPA Commission.

The Commission recommendations on public education, consumer empowerment, law enforcement, and industry call for action were crafted out of hard evidence, thoughtful concerns from various viewpoints, and were agreed to unanimously by conservatives as well as liberals on a Commission crying for solutions to a deepening dilemma while wanting to protect First Amendment rights all Americans cherish. We knew we could not keep and eat our cake simultaneously, but we wanted to provide observations, evidence, and recommendations worthy of a Congress seeking input and a nation wanting answers.

The Commission dealt with an industry growing at an alarming rate, technology changing daily, and children more knowledgeable about the internet and how it is accessed and used than parents who grew up in a simpler world. I especially offer recommendations 1 and 2 to all interested in the solution to this dilemma. This is not a problem that can be solved by parents alone—parents both of whom might be working (if there are two parents) and whose children have access to the internet at home, in school, at the home of a friend or caregiver, or home alone without parental supervision. Neither is it a government alone dilemma to solve. Yes, the government is concerned and can help, but the solution to this problem must be found in a forging of parental and government activity. Government needs to undertake a public awareness campaign, and parents need to learn more about technology and the internet. One cannot remain untutored and hope to make a difference. One cannot say: "don't do this" or "don't do that." Those are

commands signifying fury without knowledge, blind utterances without understanding.

On the other hand, government and industry have to shed adversarial roles and work together to promote acceptable use policies. The government cannot do this alone: neither can one expect industry to go it alone if government cares not to help. It is to industry's benefit to labor long and hard to end child access to pornography—a goal sought by parents—and a goal that will clearly forestall a stream of government laws and policies that hurt an industry that seems not to care about the public good.

Though the short road just trod by the COPA Commission was a difficult one, it was illuminated by a talented, caring Chairman, Donald Telage, talented and responsible fellow Commissioners whose energy was amazing and whose abilities would grace any Commission, and a Dittus staff that deserves applause and deep appreciation. I would like individually to single out five individuals who helped me greatly; Senator Conrad Burns, who nominated me for membership on the Commission, Brett Scott, President of Capital Coalitions in Washington, D.C., Todd Capser, Executive Director of the Rocky Mountain Technology Foundation in Billings, Montana, Susan Stewart, the College's Controller monitoring a COPA restricted account housed on our campus, and Suzanne Dierenfield, an Administrative Assistant without peer in my office. They offered guidance, sound advice, and much work as I made my way forward in the good work of a fine Commission which, too, deserves applause.

Commissioner J. Robert Flores, Esq.
Vice President and Senior Counsel
National Law Center for Children and Families

This Commission was tasked by Congress to evaluate technical and non-technical means of protecting minors from harmful to minors (HTM) material. Congress did not ask the Commission to recommend new legislation or comment on the COPA's constitutionality. The fact that the Commission did neither should not be construed as anything except our adherence to our Congressional mandate. Though we accomplished a great deal, the lack of federal funding made it impossible to conduct independent evaluations of technologies or industry claims. Nonetheless, the Commission made a number of findings in areas that have been the subject of endless debate. It is that accomplishment, I trust, that will enable Congress to move forward to assist parents, communities, and others to protect children.

The Commission received testimony on the effectiveness of filtering, blocking, and monitoring technologies. Librarians, parents, and business executives, who use or produce such products, convincingly demonstrated that the use of these technologies will reduce exposure to pornography. Though none of the technologies, either alone or in tandem, provides perfect protection, we do not live in a world where either the law or reality permits or encourages only perfect solutions. Moreover, the record before us demonstrates that past criticisms of filter technology are no longer valid in light of improvements in accuracy and customizability. Today, there is no basis to believe that the user of these tools will not be able to access a chicken breast casserole or get directions to Middlesex County.

Some have attempted to assign total responsibility for protecting children from HTM material to parents. While I agree with the premise that I, as a parent, am responsible for my children and their welfare, those who furnish HTM material also have an obligation to take reasonable steps to protect children. I am entitled to expect my children will not be targeted for exploitation or abuse.

The Commission heard testimony about three current technologies that can effectively be used by distributors and providers of HTM material to protect children: self-labeling, age verification IDs, and Age verification Credit

Cards. While the effectiveness and accessibility of these technologies may vary in particular settings, the Commission found that self-labeling would satisfy the criteria to be treated as an affirmative defense. Congress's decision to identify the other two technologies as affirmative defenses is supported by Commission findings that both ranked high in their effectiveness at keeping minors away from HTM materials.

Witnesses from the law enforcement community were unanimous in their belief that those engaged in the distribution of hard-core pornography, child pornography, and HTM materials do not believe they will be caught or prosecuted. FBI, state, and local officials told this Commission that the risk to children using the Internet of sexual abuse or exploitation continues to grow. Most chilling, is that the situation has gotten so bad that law enforcement is now forced to pursue only those cases where a child is being stalked.

This situation of limited law enforcement action has paralleled an exponential increase in Internet available obscenity. This material is now marketed in ways that make it nearly impossible to avoid. Pornographic spam, mousetraps, and other deceptive practices that have gone unpunished with the exception of recent FTC actions, have contributed to the mentality that "anything goes," on the Net. Law enforcement's inaction on this issue has sent the unintended message that if you are not involved in stalking children you are safe. That message also contributes to the notion that child pornographers and pedophiles can hide among the pornographic flotsam and jetsam, sending obscene e-mail and instant messages, and looking for children to exploit.

The Commission recommends launching an aggressive effort to address obscenity on the Internet because it is clearly linked to the problem of HTM material. This effort may be initiated using existing laws, is targeted at a narrow category of material, and sends a significant deterrent message. As a former prosecutor, I believe that without a credible threat of prosecution the distribution of illegal obscenity on the Internet will not diminish.

There is no way to restore innocence lost and a diet of pornographic fare will lead to disasters in fighting sexual harassment, STDs, and sexual or domestic violence. Congress, parents, other adults, and certainly the pornography industry must take steps to stop our children from being hurt. If we fail to act, our children will be right to blame us for what we have allowed.

The work of any commission depends greatly on the quality of its staff. I would like to thank Chadwick L. Groover, counsel at the National Law Center, for his extraordinary contributions to the report and the Commission's success.

Commissioner A. F. Ganier, III
CEO, Education Networks of America, Inc.

My focus during the Commission hearings has been on this country's approximately 53 million k-12 children and their 50 million parents.

While a great deal of the testimony and debate presented to the Commission revolved around the home and parents, it is clear that the schools and other public centers in America's communities have a special role to play in the next generation's adoption and utilization of the Internet. Unlike television, which was introduced into the home and never meaningfully penetrated schools and libraries, the Internet has quickly become a reality in these places. Indeed, it is estimated that our schools currently have installed 7,500,000 Internet-connected computers. This number is expected to double over the next few years.

And with good reason. Computers and the Internet represent educational tools of enormous value. Technology, if properly incorporated and used, really does have the ability to transform education. Moreover, the ability of an individual to understand, develop and use technology effectively will be critical to his or her ability to succeed in the world and to the country's continued economic development.

While many of the Commission's recommendations, such as parental education and posting information on the Web are laudable, they do not address the more than 50% of children who do not have access to technology in their homes or whose parents have no inclination towards technology. Government must continue to focus on what is going on in the schools. I estimate that Federal, State and Local governments invest more than $12 billion on Internet connectivity and related technology each year. Most of this connectivity, however, has been for connectivity's sake. The truth is that the corresponding bandwidth and hardware are not being used for productive educational programs.

One of the ways to move from the mere ability to access the Internet to the ability to enhance education is to ensure that all public places that offer Internet access to our children also offer them a safe experience. Without safety, there will be no Internet experience. Localities that find themselves

confronted with online predators and other HTM material will continue to turn the computers off and let their children fall further behind the digital divide.

Moreover, safety solutions must work transparently in order to be of real value. I personally offer low scores to many of the solutions presented because they do not work for parents, children, teachers, administrators and other members of communities that do not have the high tech skills or the inclination towards technology that such solutions require. Most policy decision-makers have almost no exposure to communities of this nature, and their recommendations therefore tend to focus on well educated communities that have high tech skills, plenty of money, and families with the time and energy to work with kids on a one-on-one basis. This is contrasted with communities where low education levels, low incomes and cultural barriers do not lend themselves to technology adoption. The goal is to break this pattern.

Finally, it should be noted that the safety of our children does not come at the expense of the First Amendment. The real barrier to free speech is that the Net is unsafe for children and, therefore, decision makers are refusing to let it be used. The baby is being thrown out with the bathwater. This is especially true in communities where the need is the greatest.

Moreover, public institutions have limited resources and enormous missions to accomplish. The responsibility of a librarian or a teacher to select how to allocate available bandwidth is no different than the decision as to how best to fill a limited number of bookshelves. There are only so many units of Internet access per dollar available. Technology permits these decisions to be made.

The conclusion that I offer the Congress is that no one solution will solve all of the problems. A combination of approaches will be required. However, any such combination must focus on schools and work in the poorest and most technologically illiterate areas. Only once this philosophy is adopted will long-term solutions such as educating 50 million parents, or encouraging them to visit a web page about safety and take the time to transfer that knowledge to their children, actually work.

Every year a whole generation of children whose parents do not have the resources or the inclinations to expose their children to technology are left further behind. The schools are where these children will find digital equality, and safety must, therefore, begin there.

Commissioner Donna Rice Hughes
Author, Kids Online/Founder, Protectkids.com

It has been a privilege to serve on the Child Online Protection Commission, and I am grateful to Senator Trent Lott for giving me this opportunity. I applaud the efforts of each Commissioner, especially the leadership of Chairman Don Telage, in building a solid foundation of unanimous recommendations to better protect children in cyberspace. I also wish to thank my client, FamilyClick and their staff, specifically, Ken Baker; Enough Is Enough; and my dedicated assistant, Judy Hyon.

Since its onset in the early nineties, the online porn industry has grown to $1.5 billion annually (Forbes, 14 June 1999). The result - today's generation of children can, intentionally or accidentally, easily access child pornography, prosecutable obscenity and harmful to minors (HTM) material. The Commission heard testimony from the National Center for Missing and Exploited Children, that one in four youths ages 10 -17, reported an unwanted exposure to online pornography in the past year. The Commission's report, which fully complements COPA, emphasizes the importance of multiple efforts on different fronts to make the Internet safer for children. This supports my belief that a three-prong solution, involving a shared responsibility between the public, the high-tech industry, and the legal sector, is essential to protect kids online.

Law enforcement officials testified that few, if any resources, have been devoted to the prosecution of obscenity. As the problem has gotten worse, the focus of prosecution has been narrowed only to those who stalk children online or produce large quantities of child pornography. The failure to adequately enforce child pornography and obscenity laws has led to a pervasive "anything goes" mentality by online pornographers and sexual predators. Our recommendation for Law Enforcement action is critical to curbing the sexual exploitation of children online. Aggressive prosecution will not only minimize children's direct exposure to online porn and sexual predators, but also decrease the sexual abuse of children by those acting out behavior depicted in pornography. Finally, the compliance of Internet Service Providers with current law should be enhanced by my recommendations of an ISP "best practices" code and the utilization of the master list of convicted pornographic sites provided by law enforcement.

The recommendation for the adult online industry to implement readily available, age-verification technologies also supports COPA. Since commercial sites already utilize some form of online payment, efforts such as credit card verification, serve to shield kids from free pornographic teaser images. While supporting the Commission's recommendation for the adult online industry to voluntarily protect children from HTM content, I am skeptical of industry-wide adoption, since, to date, the "e-porn" industry has not responded to self-regulation.

I believe there is a role for additional government regulation, even if COPA is upheld. Because COPA addresses only commercial HTM providers, I support a mandated HTM label, which the Commission found would be effective. Noted First Amendment attorney Larry Lessig, in a memorandum to the Commission, recommended such a proposal and stressed that it "provides an affirmative reason to prefer regulation over doing nothing." Additionally, a diverse panel of experts in Hearing One agreed that if HTM content were placed in a new top-level domain (gTLD) to the exclusion of other domains, and such action constituted an affirmative defense under COPA for non-obscene HTM material, it could be effective in zoning sexually-explicit content.

Witnesses before the Commission made it plain, that while there are a tremendous amount of Internet safety information and resources available, permeation into most communities has been insufficient. The Commission found that increased awareness efforts are a critical need. For maximum offline and online impact, a large scale, multi-media campaign should balance both Internet benefits and dangers. Internet 101 basic training and the implementation of effective safeguards should be encouraged in the home, school and library settings.

Technological solutions such as flexible, customizable filtering tools were found by the Commission to be very effective in preventing children's access to inappropriate content originating both in the United States and abroad. Based on Hearing Two testimony, safety rules without software tools leave an open door for children to access pornography. Testimony showed that schools and libraries that install customizable filtering software to complement their acceptable-use policies and avoid providing publicly funded peep shows for kids, were successful.

The valuable work that we achieved, in spite of time and funding constraints, further convinces me that the Commission should continue in order to build on the extensive groundwork provided by this record and report. We have an unprecedented opportunity to make the Internet safe and rewarding for children.

In only a few mouse clicks, children can be exposed to material that can never be erased from their minds. Never before in the history of telecommunications has an entire generation of children been invaded by sexually-explicit material with so few restrictions. It is incumbent on parents, industry and government to work together to provide children the protected space of innocence they deserve. Innocence lost can never be regained. The time to act is now.

Commissioner William M. Parker
CEO and President
Crosswalk.com, Inc.

Because there is so much that can be done by Government and industry to improve the protection of our children online, I feel confident that the recommendations that we have made will make a big difference if promptly implemented. They represent a first step.

When I joined this Commission I recognized the threats to our children online, and because of those threats initiated a free filtering alternative on Crosswalk.com to protect children wherever they surfed on the Internet. But as a result of my work on this Commission, I'm even more concerned about the vulnerability of children in cyberspace. Given the dangers, I must say that the time and resources given this Commission for this important task were disappointing. A task scoped to require two years by the statute was hurried to completion in six months, and with no funding. I consider this to be a credit particularly to our chairman, Don Telage, but I feel strongly that our Congress should have provided the needed time and money. Given Congress's lack of attention, or will, in this regard, I sincerely hope that the recommendations of this Commission will not similarly languish.

Furthermore, this Commission could have done much more to assist the Congress given time and money. Although the recommendations of the Commission are sound, more could have been done, and indeed, more needs to be done. The fact that the Commission is not recommending new substantive means to protect children should not be assumed to indicate that new substantive measures should not be taken. The work of the Commission to date has been merely to point out the obvious measures for which there is broad consensus and that should be taken immediately. The Congress should immediately initiate another commission, or reconvene this one, to pursue these possibilities.

I feel that the technology is available, or can be integrated, to effectively protect our children online. I particularly think that first party labeling, combined with other browser filtering technology has the promise to protect children and provide an affirmative defense to COPA, while not violating first amendment rights. The Commission did not have the time or money to

effectively pursue this potential alternative or others. Unfortunately, this Commission only progressed to the point of conducting a technology overview. We did not systematically examine technology. We did not effectively consider combinations of technologies. And we did not establish objective criteria for weighing technological approaches or methods against first amendment issues. We relied upon the testimony of vendors regarding their products. We did no testing, and we conducted no analysis of technology integration.

All that being said, there clearly is much action that can be taken now by the Government to make parents and children more aware of online dangers, and to make illegal pornographers and child abusers fearful.

Many parents and children simply are not aware of online dangers. And while many in the Internet industry are fearful of scaring people off the web, a comprehensive program to inform the general public of the dangers of the Internet must be initiated. The dot com advertising blitz is more than sufficient to inform the public of the great promise and opportunity associated with the Internet. The Government cannot remain silent about the clear dangers of this medium, particularly for children, and particularly while there are no current effective safeguards for them. This public awareness campaign must be on a scale with Government campaigns to warn of other dangers, with an objective that every parent be aware of the need to engage to protect children online. This public awareness campaign must be complemented by an education program sufficient to provide those parents (and children) with the information they need for effective protection.

While this is a complex problem, I was appalled at the almost total lack of enforcement of existing obscenity law. The adult entertainment industry is almost boastful about the neglect of law enforcement officials that they currently enjoy. Several witnesses testified that producers of obscene and "harmful to minors" material have no fear of prosecution. There is currently very little funding to pursue violations of current statutes, and there is no coordinated law enforcement strategy (and effort) being pursued by the federal government. Congress must give the Justice Department an aggressive mandate and funding to enforce existing laws.

If the Congress decides to re-establish and fund this Commission consistent with the intent of the statute, I would be honored to serve again as a Commissioner.

Commissioner C. James Schmidt
Professor
School of Library and Information Science
San Jose State University

It has been said that the Internet is a "world-wide conversation". There is no limit to the number who may speak, the admission price for speakers is low, users can seek and "hear" the speech of their choosing.

As is the case with the printed medium, where the cost of speaking – publishing – is higher, the Internet's world-wide conversation contains speech offensive to some.

Congress asked the Commission established by the COPA legislation to examine ONE facet of this world-wide speech – content which might be or is "harmful to minors" – and to recommend ways in which minors might be protected from such content.

I did not enter into our task confident that the Commission could identify a constitutionally permissible way for American intervention into this world-wide conversation. A previous Congressional attempt to regulate content on the Internet – the Communications Decency Act – was declared by the Supreme Court to be unconstitutional. Attempts by several states to regulate content on the Internet including harmful-to-minors material, e.g. Michigan, New York, Georgia, New Mexico, Virginia, have also been nullified by the courts. And a portion of the COPA legislation itself, aimed at regulating content, has been temporarily enjoined by a federal district court, and that enjoinment has been upheld on appeal.

However, the decisions of American courts are only a part of the story, since the Internet, by action of the Congress in 1998, is now subject to international governance through ICAAN. Therefore, enforcement of content regulation on the Internet in many instances will require multinational agreement – on definition of content, on reciprocity, on extradition, etc. Analogous difficulties, mitigated by some agreements, exist with respect to enforcement of laws about narcotics, currency transfers, terrorism, etc.

In the end, the protection of minors from Internet content that may be harmful to some will require active adult supervision. "Too much to do and too little time" is the response from many parents, guardians and care-givers. Hence a massive educational effort is needed, combined with the development of easily accessible tools, so parents and kids can participate in the world-wide conversation and realize the benefits while feeling safe.

The educational effort proposed is urgent and will be expensive. The urgency arises in part from the rapid growth of content – innocuous as well as offensive – on the Internet and the Web. Millions of web pages added each week. Web sites appearing and disappearing. The world-wide conversation has new speakers every second and content which appears and disappears with the speed of light. Urgency also arises from pervasive access. Schools are wired, classrooms are connected, ninety-five percent of American public libraries provide Internet access to their patrons. And then there is the wireless revolution, with broadband wireless – sufficient to carry broadcast quality video – just months away from introduction to consumers in Japan. A child who can't access certain content because of adult supervision or protective technology tools at home or school may easily access such content with a friend's wireless device in the backyard, on the bus, or while walking. Not many months away, Internet access won't require a home or school or library computer connected to a cable but rather a cheap and easily portable device.

The expense of the proposed educational effort owes to the need, first, to overcome adult fears of a medium – the Internet – which many know less about than the minors entrusted to their care. There are some simple rules for the electronic highway, which kids should be taught and which have their analogs in the physical world. "Don't accept a ride with a stranger"; "Don't give out your address or phone number to strangers"; etc. Second, besides reaching large numbers of adults in many languages, the educational effort must be sustained over time. Such efforts have been undertaken with respect to smoking, tobacco products and kids, alcohol and pregnancy, seatbelts.

To assure participation by all in this world-wide conversation, education is needed where law cannot reach.

A note about law enforcement. Testimony and submissions to the Commission's record were clear on two points. First, vigorous prosecution of Internet content under existing obscenity and child pornography statutes does not have a high enough priority. Secondly, law enforcement, especially at state and local levels, lacks the tools and the skills to investigate such crimes. Significant new resources will have to be provided to all levels, especially state and local.

Commissioner William L. Schrader
Chairman and Chief Executive Officer,
PSINet Inc.

I commend my colleagues on the Commission for striving wholeheartedly toward consensus. Our respective viewpoints are very different, but at every turn the Commission moved away from polarization and discord so that, as a body, we could bring forward a set of recommendations with the weight of unanimity behind them. This is no small achievement and I am proud to have been a part of it.

The problem the Commission was asked to address – how we can protect our children from exposure to the grotesque images that are the stock in trade of the "adult content industry" on the Internet – does not admit of a one-dimensional solution. The law that brought this Commission into being, the Child Online Protection Act ("COPA"), shares the characteristics of other "magic bullets" – most are superficially appealing but deeply flawed. I believe, like several other members of the Commission, that the restrictions on speech enacted into law by COPA are unconstitutional. Participating in the work of the Commission has only brought into sharper relief the fundamental obstacles to legislating our way out of the problem.

One of the hard truths that complicates legislative efforts is that material that is "harmful to minors" (as legally defined) is not limited to the puerile, pornographic output of the "adult content industry." There is a wealth of content on the Internet that is sexually explicit but valuable (and therefore lawful) for adults – from the standpoint of literary, scientific, artistic, and even political values. Measures that are entirely appropriate to suppress the availability to minors of content purveyed by the "adult content industry" often have decidedly adverse impacts on the ability of serious-minded authors, educators, artists, or journalists to reach their intended audience via the Internet. For this reason, I believe there is *no* single, one-size-fits-all, technological equivalent of a "brown paper wrapper" in this new medium.

As PSINet has joined in legal actions to overturn recent "harmful to minors" enactments by State legislatures, I have found it instructive that none of the other plaintiffs can be considered purveyors of porn. Instead, they include sex educators, authors and publishers of controversial literary or artistic works, and AIDS activists. I do not doubt that much of the material published on the Internet by these content providers may meet the legal definition of "harmful to minors," especially for younger minors, for whom the

educational or artistic value may be beyond their comprehension. To suggest, however, that these authors should be forced *by law* to segregate their work behind a credit card or age verification barrier, or label it as part of a new ".XXX" domain, or require that it be "X-rated" in a manner similar to adult movies and videos, illustrates how troublesome it is to apply these measures to the exceptionally diverse range of lawful content that may be "harmful to minors."

Wisely, the Commission recommends that only the "adult content industry" – not all authors or publishers of "harmful to minors" content – adopt certain of these measures, and that they do so voluntarily, as part of a self-regulatory regime and not as a legal mandate enforced by the threat of criminal prosecution.

The other hard truth that vexes our efforts is a constitutional one – that the ultimate legal judgment of content as "obscene" or "harmful to minors" can only be made in the context of local community standards. For this reason, I had suggested that the Commission call for a public dialogue, including lawyers, advocacy groups, and academics, on the constitutional question whether it is possible to reconcile First Amendment obscenity jurisprudence with the technological fact that the "community" of speakers and listeners on the Internet is inherently global. The Third Circuit Court of Appeals in Philadelphia held that, in enacting COPA, Congress recognized this conundrum but tried (unsuccessfully) to sidestep it. My concern is that, while encouraging stepped-up efforts at prosecution of obscene content, the Commission has perhaps glossed over the difficulties prosecutors may face in obtaining convictions, and sustaining them against challenge, for obscenity in a medium that (unlike any other in history) enables anyone, anywhere, to be both a "publisher" and a "listener" in a community that knows no geographical bounds.

For these reasons, I applaud the Commission for embracing solutions that rely primarily on educating and empowering parents and caregivers to protect children, while setting aside proposals for content-based legislation that would not only fail to protect children but would threaten the robust First Amendment protection that federal courts at all levels have extended to the Internet.

Commissioner Laurence Shapiro
Executive Vice President
Walt Disney Internet Group

Upon careful consideration, I have come to the conclusion that a variety of measures – as opposed to any singular measure – must be supported in order to effectively protect children from harmful material on the Internet. I believe that it is also important to note that there is no single or combined pure technological solution to protecting children from harmful materials. Indeed, I believe that all the measures and resources imaginable will never be an adequate substitute to homes where parents are fully involved in the online activities of their children. In order to provide parents with the necessary assistance to guide their involvement, these measures should primarily include a significant new public education campaign geared towards educating parents and their children of the growing resources available to protect children from harmful materials. These measures should include easy-to-use and –find online tools that parents can use to ensure that their children avoid harmful material. In addition to these educational efforts, the Commission heard clear evidence that efforts to protect children from harmful materials should include heightened enforcement of existing laws against child pornography and obscenity and I fully support the recommendations of the Commission in this area.

It is important to note that these measures must be undertaken with cooperation not only between the private and public sectors in the United States but also throughout the world. The Internet is a global medium and its problems must be handled as such. While we have been charged with reporting back to Congress on how to protect children from harmful material online, we must be mindful that domestic solutions alone will never fully resolve international problems.

As an executive with The Walt Disney Internet Group, I can report that we are trying to do our part to protect children from harmful material through filtering tools, such as Go guardian, and educational initiatives, such as Disney's Safe Surf Island and Doug's Safety Page. We are a founding member of GetNetWise and will continue to be active in our support of industry-wide educational initiatives. In addition to the above-mentioned measures,

companies, like mine, must remain resolved in our commitment to providing safe and trustworthy online experiences.

It has been a pleasure and an honor to serve on the Child Online Protection Act ("COPA") Commission. I am particularly grateful to Congressman Richard Gephardt, the Minority Leader in the House of Representatives, for having recommended my nomination. I want to thank Chris Curtin, in the Washington office of The Walt Disney Company, for the assistance he provided to me throughout this process. Finally, I want to commend Don Telage, the Chairman of the COPA Commission, for all he did to facilitate the appropriate deliberation of these important issues.

Commissioner Srinija Srinivasan
Yahoo! Inc.

Since 1995, Yahoo! has reflected the power and potential of the Web, committed to being a fun, friendly, effective starting point for online exploration. The benefits of the Web to adults and children alike are innumerable and growing. In many cases, the Web has eliminated the boundaries of space and the limitations of time, bringing a staggering array of content, communication facilities, and commercial possibilities to anyone in the world, at any time, at the click of a mouse.

The myriad benefits of the Web are accompanied by some risks and potential dangers, however, particularly to young children who engage in online activities without appropriate supervision and education. Since the launch of Yahooligans! in 1996, Yahoo! has additionally been committed to providing a safe haven for children to explore online.

No single method or technology is a panacea for protecting children. In the "real world" we spend time teaching children to make good decisions about even seemingly simple tasks such as when and how to cross the road. The same care and attention is necessary to promote safety online. Ensuring that the Web is safe for children starts with educated and involved adults, who help children understand what's appropriate and how to avoid danger. Offline parental education resources, online one-click-away resources that highlight useful tools and technologies, and the incorporation of acceptable use policies are all highly accessible, effective methods that ensure parental involvement in children's online explorations.

Yahooligans! is built by a team of experienced educators who know how to create an entertaining, edifying experience for a young audience. Yahooligans! is full of content intended specifically for children, but the informed human judgment of the editors also allows for inclusion of a vast array of material that is age-appropriate even if targeted at a general audience. Content from sources such as the Smithsonian, the White House, NASA, or the New York Times may not fall within a limited children-only umbrella (such as a .kids domain), but greatly enhance a child's online experience. As a greenspace, Yahooligans! does not prevent children from venturing outside its walls, but by gathering and presenting a wealth of

interesting, age-appropriate material, it provides children a safe, compelling environment to keep them from seeking harmful or inappropriate material outside the safe zone.

Keeping children from seeking harmful content is a crucial component of protecting them online. Keeping harmful content from seeking or finding children is also critical to ensuring a safe environment. The former is addressed through the active involvement of parents and teachers, as well as the use of greenspaces, educational resources, and acceptable use policies; the latter can be addressed with the use of various technological aids as well as through effective law enforcement.

While technology will never be a substitute for parental involvement, and no technology will ever replace the guidance of a caring teacher, many technological solutions exist that supplement non-technological methods of protecting children. Filtering and blocking software, as well as monitoring and tracking tools, can serve to exclude harmful content, complementing areas like greenspaces that include appropriate content.

When these various methods and technologies are coupled with effective law enforcement to stop bad actors, the Web offers unlimited potential for children to enjoy a safe, rewarding, entertaining and educational experience online.

It has been a privilege to serve on the Commission on Online Child Protection. I would like to thank the Yahooligans! team for sharing their insights with the Commission, and for their infectious enthusiasm and tireless dedication to creating a fun, friendly, enriching and safe place for children to go online. I am proud to be part of an organization that helps children have a safe, rewarding web experience.

I have been honored to serve with my fellow Commissioners, and I would like to thank each of them for their hard work and dedication to protecting children online, throughout the life of the Commission and beyond.

## Commissioner Karen Talbert
## Nortel Networks

It has been my privilege to serve on the Commission on Online Child Protection and an honor to be a part of this important study. I would like to thank Chairman Don Telage and my fellow commissioners for their respect, knowledge, and thoughtful contributions, which have led to our agreement on final recommendations. Additionally, I would like to thank Amerivision Communications and Nortel Networks for supporting my participation on the Commission.

The problems and issues we have addressed concern me as a citizen, a parent and as an individual who cares about kids. Over the past few years, based upon my exposure and involvement in a wide range of Internet projects, I have had the opportunity to closely use, observe and formulate opinions regarding this resource. I have seen the problems it can create for families. I have researched possible solutions and contributed to the development of a server-based filtered product. My personal conclusions follow that of the Commission; there is no single solution, but we must continue to address the issues with a variety of solutions that exist today and make sound recommendations for the future.

We have established a solid base of information from which many solutions can be immediately implemented while setting the groundwork for the future and improvements to be built upon. We have clearly seen the safety issues and threatening situations that children can easily be exposed to on the Internet. We understand that a profoundly simple approach does not exist.

I believe the biggest risk we face, is that nothing is done as a result of our efforts. I will always remember the children who testified to their frightening experiences on the Internet. The consequences of doing nothing were clearly articulated by the testimony of experts who educated us on the dangers of harmful content and of not protecting our children, our greatest fears confirmed.

Unfortunately, statistics show that a high percentage of children are online and unsupervised while their parents are at work. I have met with many

parents who are knowledge workers during the day, but who are out of touch with what their children are seeing online in their home.

With most of my 15 years experience working in a large corporation, I am an advocate of educational programs in the workplace. Within the working environments of our country are vast resources that can be deployed to deliver information on Internet safety to working parents and employees of all ages. Government should consider incentives for businesses to educate employees as a fast and effective way to enhance public awareness.

More and more companies are becoming aware of Internet safety, security and privacy issues as they apply to the workforce. It seems a natural extension to carry that awareness a step further and educate workers on basic Internet safety. Businesses can benefit from offering training, literature, demonstrations and online information to help parents become knowledgeable about the Internet. Parents benefit from knowing how to help their kids have a safe Internet experience. I hope to see organizations embrace a commitment of "best Internet practices" to educate their workforce and adopt safety policies that can be carried over into the home.

What do YOU want the Internet to be? The question is a service mark of Nortel Networks. It is also a provocative question that we have asked ourselves many times during the course of the Commission's work. What do you want the Internet to be – for our children? Is the answer – a powerful educational resource and fun tool…or a place where kids don't feel safe, or where curious kids can lose their innocence?

It will take the efforts of everyone, from care givers of children to service providers of access and content, to have a positive impact on the problems. The dynamics of this powerful medium will continue to challenge us. Directly or indirectly, our children will continue to educate us about the good and the bad aspects of the Internet.

I challenge Congress to address the Commission's recommendations. It is my sincere hope that our recommendations will solicit specific and long-term actions that gain acceptance and momentum toward making the Internet a safer place. To keep children safe, we must persevere in finding and implementing solutions that meet and exceed the objectives of our original

charter. Our overall success will be measured by the collective willingness of government, private and public sectors to accept responsibility for addressing the problems and to take immediate action.

Commissioner George Vradenburg, III
Vice President for Global & Strategic Policy
America Online, Inc.

It has been my pleasure and honor to serve on this Commission, along with my distinguished colleagues from throughout the Internet industry and the public interest community. I appreciate their dedication and creative thinking in the critical area of keeping children's online experiences safe, educational, and entertaining. I also want to thank Elizabeth Frazee of AOL and Liza Kessler of Leslie Harris & Associates for their hard work on my behalf in support of this Commission.

This Commission has worked hard to meet the challenge Congress presented to us: evaluating technologies and methods to help protect children from exposure to harmful to minors material, and making recommendations based on our findings. We heard from producers of cutting edge technology, educators, law enforcement agents, and young Internet users.

Based on my experience on this Commission, three things stand out:

1.) Technology choices are robust and continue to develop.

We heard testimony from GetNetWise that they have grown to include over 120 parental empowerment tools. We also heard testimony from companies that analyze information on the Internet in real time, companies considering children's online safety in wireless and broadband, and companies with many creative approaches to Internet safety. None is a "magic bullet" for child safety, but each may fit the needs of some families. Furthermore, there is every reason to believe that these technologies will continue to develop and thrive.

2.) Education works.

No law, technology, or corporate initiative can take the place of an involved parent who understands the importance of exercising parental control over children online. AOL has been leader in this area, and will continue to educate children, parents, and other consumers about how to have a safe online experience, and about their choices for parental controls.

We look forward to continuing work on this with other industry leaders, educators, non-profit organizations, and especially parents.

AOL's internal effort to educate consumers about online safety, useful child-friendly content, and the Parental Controls available to them have been an extraordinary success. We believe that similar efforts must continue to take place throughout the Internet industry. GetNetWise is a good example of the kind of work that we can do together to educate families on Internet safety and their choices of parental empowerment tools. AOL will continue to promote public-private interest partnerships that focus on educating families and caregivers on Internet and online safety.

3.) Existing laws with regard to child sexual exploitation, child pornography, obscenity, and where clearly applicable, "harmful to minors," should be enforced.

Many law enforcement officers and children's safety advocates testified to the COPA Commission that they are hard at work protecting our children from sexual predators who use the Internet as a means of contacting children. They testified that police resources are stretched thin, and that they had trouble recruiting, training, and retaining sufficient officers to address this problem.

Every level of government, from Congress and the Executive Branch of the federal government on down must recommit themselves to protecting children from online exploitation, and to making resources available to hire staff, improve training programs, and foster cooperation between law enforcement agencies and jurisdictions.

This Commission examined innumerable technologies and methods for protecting children from harmful to minors material online. A well-informed parent has the power to teach his or her child the safety rules of the Internet and the power to find -- and fine-tune -- a technology that approximately reflects that family's values. Unfortunately, the kind of broad-based multi-media education that families need in order to make informed choices online does not have the reach it needs.

At AOL we have always believed that protecting children online must be a collaborative effort between families, caregivers, and the private and public sectors, including law enforcement. Particularly as technology evolves and converges, we must look together for new ways to give parents the skills and tools they need to keep up with technological advances. We all need to work together supporting efforts such as GetNetWise, educating children, parents, and caregivers about safe and appropriate online activity, and developing and refining technological tools so that families and caregivers can make informed choices about how their children use the Internet. AOL has been a leader in these efforts and will continue this leadership.

Our work together must not stop with the submission of this report to Congress. AOL is committed to remain involved in this critical national issue and to continue pushing it forward.